ciphertrust.com

December 2005

IronMail Edge® User's Guide

Product Version 1.0

CipherTrust®
Peace of Mind in Messaging™

©2005 CipherTrust, Inc. CipherTrust and the CipherTrust logo are registered trademarks of CipherTrust, Inc. All other trademarks are the property of their respective owners. All rights reserved.

IronMail Edge User's Guide

Product Verison 1.0

Table of Contents

Before You Begin ix

How This Book is Organized ix
How to Use This Book x
Conventions x
Contacting CipherTrust x

I: Getting Started 1

What is IronMail Edge? 1
In this section 2
Process Overview 3

Chapter 1: Setting Up IronMail 5

In this chapter: 5
Configuring IronMail 5
Preliminary Information 5
Initial Configuration Wizard 6
Network Connectivity 16
DNS Configuration 16
Internal Mail Server Configuration 17
Network Firewall Configuration 17
Configuring the Firewall 17

Chapter 2: Best Practices Configuration 21

In this chapter 21
SmartStart 21
Using SmartStart 21
The SmartStart Screen 22
Accessing SmartStart 23
When You Have Finished SmartStart 30

II: Monitoring the System 31

Using the Dashboard 31
In this section: 31

Chapter 3: The Dashboard 33

In this chapter 33
The Dashboard Screen 33
Configuring the Dashboard 34

Special Navigation 36
Configuring the Graphs 37
System Graphs 38
Queue Graphs 38
Executive Graphs 39
Special Navigation 39
Saving the Configuration 39

III: Encryption 41

Introduction 41
In this section 42

Chapter 4: Managing Certificates 43

Certificates 43
X509 Certificates 43
Adding a CSR 44
Installing an X509 Certificate 47
Storing X509 Certificates 48
Exporting an X509 Certificate 49
Importing an X509 Certificate 50

IV: Protection Manager 53

In this section 54
Available Reports 55
Services Status 55
Active Protection Status 56
Mail IDS Status 56

Chapter 5: Mail Firewall 59

In this chapter 59
Mail Services 59
Configure Mail Services 60
SMTPI Service 61
SMTPO Service 65
Global Properties 72
Mail Routing 76
Domain-Based Routing 76
Adding a New Routing Domain 77
Editing an Existing Domain 78

Chapter 6: Mail Intrusion Detection Service 81

In this chapter 81
Application Level Protection 81
Denial of Service Protection 81
Configuring Application Level Protection 83
Network Level Protection 85
Analysis Console 85
Configuring Network Level Protection 86
Signature Manager 89
Signature Dictionary 90
Signature Updates 91
System Level Protection 92

Program Integrity 92
File System Integrity 93
V: Reporting 95
Introduction 95
In this section 95
The Reports Viewer 96
Chapter 7: Alert Manager 97
In this chapter 97
Alert Levels 97
Alert Class 99
Adding an Alert Class 99
Editing an Alert Class 100
Alert Mechanisms 102
Adding an Alert Mechanism 103
The Alert Viewer 107
Chapter 8: The Health Monitor 111
In this chapter 111
Configuring the Health Monitor 111
Health Monitor's Tests 115
Configuring IronMail Alerts 117
Chapter 9: Advanced Reporting 119
In this chapter 119
Reports Configuration 119
Report Descriptions 123
Detailed Logs 123
Summary Logs 128
X: Administration 135
Introduction 135
In this section 135
Chapter 10: Configuring Web Administration 137
In this chapter 137
User Accounts 137
Creating User Accounts 137
Managing User Accounts 139
Allowed IPs 142
Web Admin Settings 144
User Preferences 145
Dashboard Preferences 145
Chapter 11: General Administration Functions 149
In this chapter 149
The Cleanup Schedule 149
Configuring Appliance Certificates 152
Changing the Admin Password 153
SmartStart Configuration 154

VII: System.....155
In this section 155
Chapter 12: System Configuration 157
In this chapter 157
Appliance Configuration 157
Out-of-Band Management 160
Routing 162
The Serial Port 163
SSH Configuration 164
System Backup 166
System Restore 168
The Check Tool 170
Chapter 13: System Updates 171
In this chapter 171
Software Updates 171
Product Updates 171
Hotfix Updates 173
Applying the Updates 174
Threat Response Updates 176
TrustedSource Updates 176
Configuration Updates 178
Mail-IDS Updates 179
Configuring Auto-Updates 181
License Manager 182
Chapter 14: General System Functions 185
In this chapter 185
UPS Statistics 185
Powering Down and Restarting 186
Setting the Date and Time 187
Storing CMC Keys 189
Resetting Keys 190
VIII: Additional Functions.....191
Introduction 191
In this section 191
Chapter 15: Using the Command Line 193
In this chapter 193
The Command Line 193
The Commands 194
The HELP Command 195
The EDIT Command 196
The RUN Command 197
The SET Command 198
The SHOW Command 200
The SYSTEM Command 205
The TAIL Command 205

The TEST Command 206
The History Command 208

Before You Begin

How This Book is Organized

This manual is comprised of sections that correspond to the major program areas of IronMail, as identified by the tabs at the top of IronMail's main screen. The chapters within a section are intended to follow the organization of each area's navigation menus, which will appear to the left of the IronMail screen. Here is a brief summary of what you will find in the manual.

Section I: Getting Started

Getting Started will briefly introduce IronMail and help you perform the basic setup and configuration necessary to get the appliance deployed. The section contains the following chapters:

- Chapter 1: Setting Up IronMail
- Chapter 2: Best Practices Configuration

Section II: Monitoring the System

Monitoring the System will introduce you to the IronMail Dashboard where you can capture information at a glance regarding your IronMail's operation. The section contains this chapter:

- Chapter 3: The Dashboard

Section III: Encryption

This section is concerned with the application and management of encryption methods to provide secure mail flow. The following chapters are in this section:

- Chapter 4: Managing Encryption

Section IV: Protection Manager

Protection Manager includes discussions of network security and intrusion detection and prevention. The following chapters are included:

- Chapter 5: Mail Firewall
- Chapter 6: Mail Intrusion Detection Service

Section V: Reporting

Tracking the operation of the IronMail system and accessing necessary levels of detail regarding its performance are essential. The Reporting section discusses means for monitoring whatever detail is required. The following chapters are included:

- Chapter 7: Alerts Manager
- Chapter 8: Health Monitor
- Chapter 9: Advanced Reporting

Section VI: Administration

The Administration section discusses the methods for configuring access to the IronMail appliance as well as the routine self-monitoring by the system and the alerts that may result. The section contains the following chapters:

- Chapter 10: Configuring Web Administration
- Chapter 11: General Administrative Functions

Section VII: System

The System section is concerned with the functions necessary to set up and maintain the IronMail system, keeping it up to date and effective. The following chapters appear in this section:

- Chapter 12: System Configuration
- Chapter 13: System Updates
- Chapter 14: General System Functions

Section VIII: Additional Functions

This section provides information regarding less commonly-accessed functions of IronMail. The following chapters are included:

- Chapter 15: Using the Command Line

How to Use This Book

This manual should have been delivered to you in two formats: PDF and Compiled HTML. You can navigate through the manual by clicking a line in the Table of Contents (each line is a hyperlink to the page it references). The same is true of the items in the Index.

Conventions

Names of command buttons or other items you may access from the screen will appear in **boldface** type. Examples: **Submit** - **Next** - **Reset**.

Navigation that will take you to the screens you see in this manual is shown in the left margin. The navigation text appears in a ***Boldface Blue Italic*** font. Example: ***Queue Manager > Outbound Queues > Current Messages***.

Contacting CipherTrust

If you have questions or need assistance, you may contact CipherTrust using the following information:

Phone: 1-(877) 448-8625

Website: www.ciphertrust.com

I: Getting Started

What is IronMail Edge?

The IronMail Edge e-mail security appliance was designed specifically to address the issue of rising e-mail volume. IronMail Edge is positioned at the perimeter of the mail system, controlling traffic at the network border, rather than at the mail server or desktop.

CipherTrust has designed IronMail Edge with a hardened operating system, a proprietary MTA and a Mail IDS (intrusion detection system). What this means to an organization is that IronMail Edge can safely be placed at the network edge to perform its role. IronMail Edge does not rely on any commonly used MTA software, as many of those are known to have vulnerabilities. Additionally, IronMail Edge will block hacker attacks that use methods such as denial-of-service attacks (syn flood), Telnet or ping attacks, and buffer overflow attacks.

IronMail Edge relies on TrustedSource, CipherTrust's revolutionary reputation system, for information about every sender that attempts to connect to the protected enterprise's mail servers. TrustedSource is the first and only reputation system to combine traffic data, whitelists, blacklists and outbreak detection with the unparalleled strength of CipherTrust's global customer network of more than 1600 customers in 40 countries, including over one-third of the Fortune 500. It is also the only reputation system available that is able to provide numerical scoring for every IP address across the Internet (approximately 4.2 billion).

When the IronMail Edge appliance receives an SMTP connection request, the box will hold the response to the sender until the sender reputation is understood. IronMail Edge utilizes the intelligence provided by TrustedSource to make high-speed decisions about whether messages should be rejected or allowed, based on a quick IP lookup operation. IronMail Edge maximizes speed and efficiency by caching

the TrustedSource data locally, with regular updates streamed from the central TrustedSource server. Using the TrustedSource data, IronMail Edge can take any of the following actions:

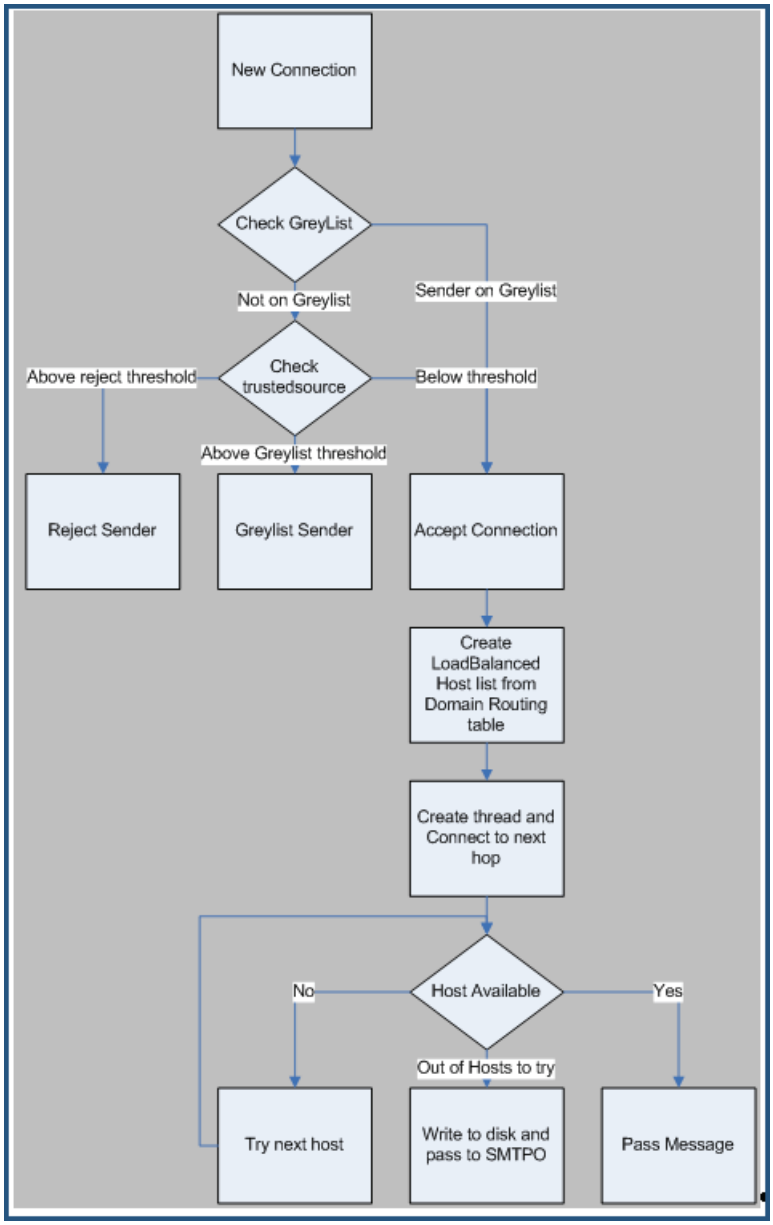
- When IronMail Edge receives a connection request from a known bad sender, such as a spammer or hacker, it rejects the connection immediately without accepting any data into corporate network. The sender receives an error code telling them not to retry the connection, as it will only lead to another rejection.
- When a sender receives a score from TrustedSource that falls into the "suspicious" range, IronMail Edge will again reject the connection, but will ask the suspicious sender to retry. This traffic shaping, or throttling, is very effective in slowing down the volume of bad e-mail. Legitimate senders will receive the request and resend the message, which will then be accepted. Conversely, spammers, phishers and the like typically will not retry; re-sending mass quantities of messages is expensive, and their mass-mailing programs are not written to include "retry" logic.
- Messages from "good" senders will pass through the IronMail Edge box to the mail server without any processing. IronMail Edge will not acknowledge to the sender that the message has been received until the mail gateway confirms it has received the message.

In this section

In this section, you will find the following chapters:

- Chapter 1: Setting Up IronMail
- Chapter 2: Best Practices Configuration

Process Overview



The flow chart above illustrates the IronMail Edge process. The steps in the process are as follows:

IronMail Edge Processing

Step	Action	Description
1	Edge receives a new connection.	A connection is attempted for incoming mail via SMTPI.

IronMail Edge Processing

Step	Action	Description
2	Edge checks the Greylist	If the sender is not on the Greylist, Edge proceeds to the next step. If the sender is on the Greylist, Edge accepts the connection.
3	Edge checks the sender using TrustedSource.	If the sender's TrustedSource score is above the rejection threshold, Edge rejects the connection. If the score is above the Greylist threshold, Edge Greylists the sender, requiring the sender to try again for connection. If the score is below the thresholds, Edge accepts the connection.
4	Create the host list	When a connection is accepted, Edge creates a load-balanced host list from the Domain Routing table.
5	Create thread and connect	Edge creates a process thread for the message and attempts to connect to a host.
6	Determine host	If the selected host is available, Edge passes the message to that host. If the host is not available, Edge will try the next host. If, and only if, no host is available, Edge will fall back to writing messages to disk and passing them to SMTPO to be sent to a host when one is available.

Setting Up IronMail

The initial setup for IronMail includes at least two major components, and possibly a third. The Installer or Administrator must set up the basic IronMail appliance to allow its further configuration after the basic initialization is completed; they must also perform essential setup for connectivity to the internet and to the mail network. The third component is necessary only if the IronMail appliance is being set up as a Centralized Management Console (CMC).

Setup results in only the most basic configuration of IronMail. Once all initial setup is complete, the Administrator will perform the detailed configuration that prepares IronMail to protect the specific network.

In this chapter: In this chapter, you will find information about the following topics:

- Configuring IronMail
- Running the Installation Wizard
  - Configuring IronMail as a CMC
- Network Connectivity
  - Configuring the Firewall

Configuring IronMail

Preliminary Information

IronMail—whether intended as a stand-alone appliance or as a Centralized Management Console—uses a simple wizard to set the initial values required for it to become minimally functional. Before you run the wizard, obtain the information requested in the form below. Your network administrator should be able to assist you in determining the network information. (A copy of this Information Gathering Form appears at the back of the Setup Guide so it may be removed for easy information gathering.)

1. Have on hand the License Key that was e-mailed to you for the IronMail appliance. The License Key contains information that determines whether this appliance is a Centralized Management Console for enterprise environments or a stand-alone IronMail.
2. Create a host name for this appliance.
3. Determine the domain name to which this appliance belongs.
4. Assign an IP address for this appliance.
5. Determine the Subnet Mask for this appliance.
6. Specify the Default Router the appliance will use.

7. Specify the IP Address of at least one of your DNS Servers (This appliance must be able to connect to it.)
8. Provide the fully qualified domain names of up to three Network Time Protocol servers. (IronMail identifies three servers by default.)
9. Specify the appliance's time zone by selecting from the pick list the city nearest the appliance. (The selected city must be in the same time zone as IronMail.)
10. For "stand-alone" IronMail only! — Specify the fully qualified domain name of your default mail server. (If you have dedicated servers handling incoming and outgoing mail, or other services, select one to enter during the wizard setup—the remaining servers will be configured later.) This information is not necessary for configuring a Centralized Management Console.
11. Specify the IP address of the default mail server you identified above.
12. Specify your default email domain.
13. Determine if you want IronMail to use secure POP3 or IMAP 4 with your internal server. (Your internal server must have a Security Certificate installed on it for secure POP3 or IMAP4 to be implemented.).

Verify this information with your Network Administrator prior to running the appliance's Initial Configuration Wizard.

Initial Configuration Wizard

IronMail ships with a pre-installed, albeit unsigned, Security Certificate. IronMail only allows administrative sessions with it over a secure SSL (https) connection, for which a Security Certificate is required. The default Security Certificate is adequate for creating these secure connections from your browser to the IronMail appliance, but is not adequate for providing SSL security for your email infrastructure. Until you install a valid Security Certificate from a Certificate Authority, your browser will display a Security Alert each time you logon to the appliance. Clicking **Yes** at the prompt allows you to proceed.

You must connect to the appliance to enter some preliminary values in an Initial Configuration Wizard in order to make the appliance initially functional. Use a client workstation (any Windows PC) as IronMail's "front end." There are two ways you can connect to the appliance:

- Use a network "cross-over" cable to physically connect a PC workstation to IronMail. (The cable plugs into the network port on each device.)
- Install IronMail in your existing network, but set a PC workstation's netmask to match IronMail's default IP address and netmask.

For either type of connection, the client workstation must temporarily change its IP address and netmask to match IronMail's default values

(IP Address: **192.168.0.254**, Netmask: **255.255.255.0**). That is, change your workstation IP address to 192.168.0.xxx, and the netmask to 255.255.255.0 (where xxx is any number between 0-253).

1. Launch Internet Explorer on the client workstation and navigate to IronMail's built-in default IP address:

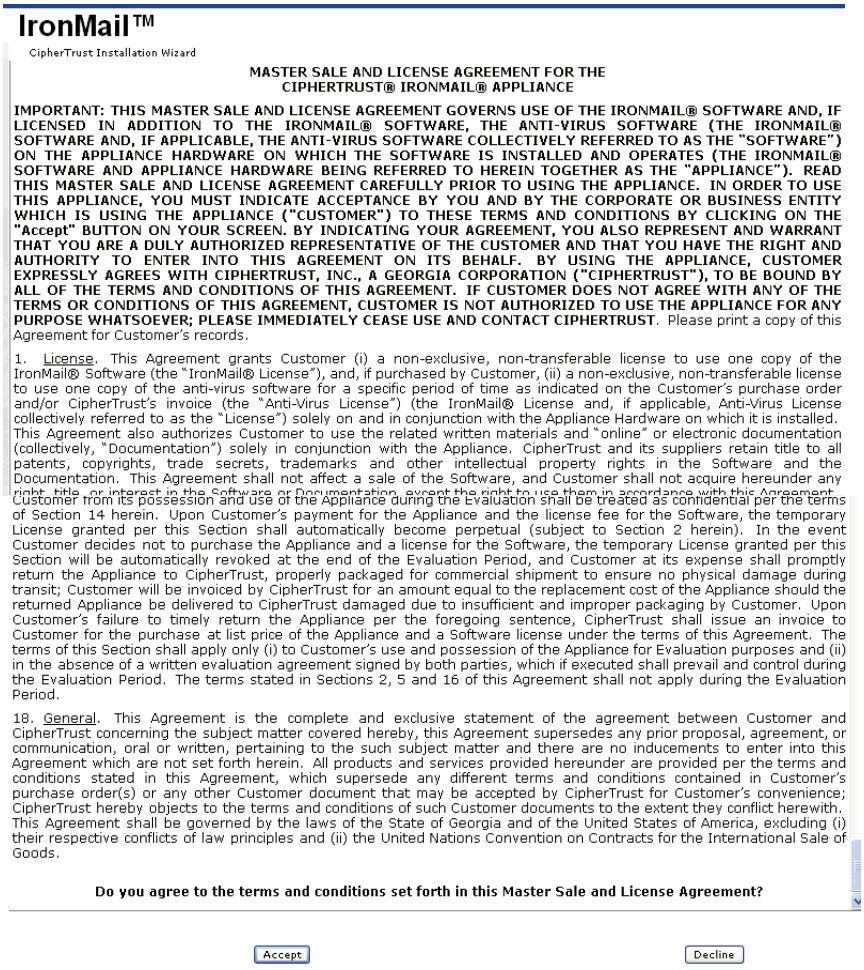
   https://192.168.0.254

   You must add the letter "s" after "http."

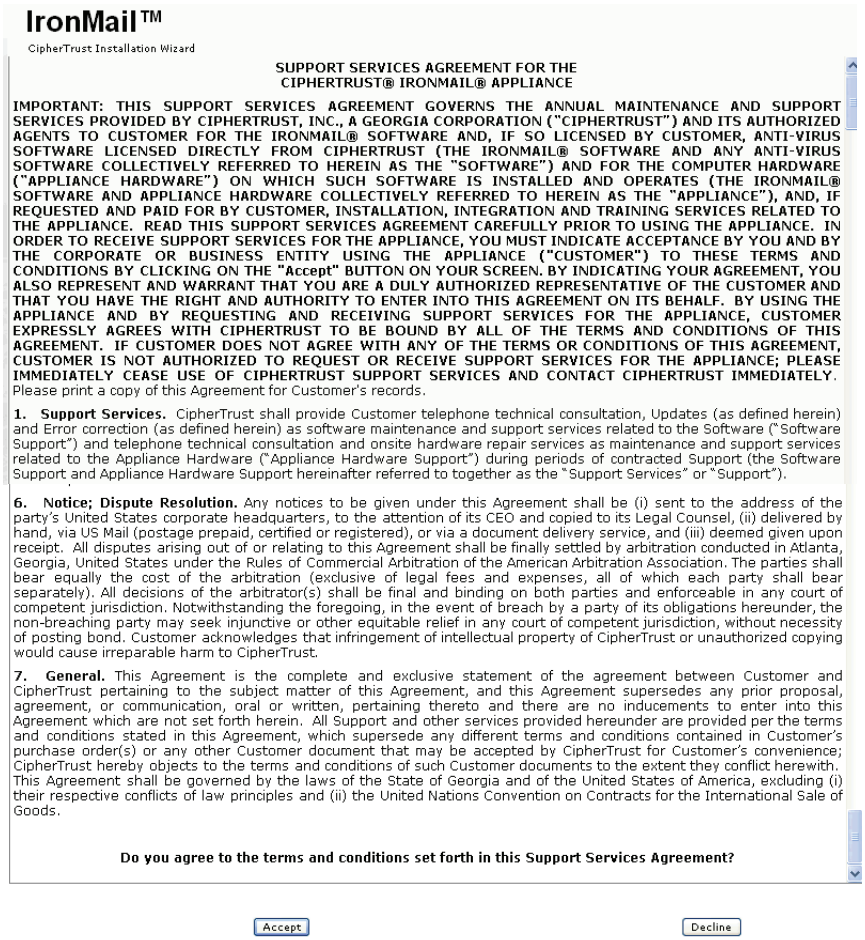
   The opening screen for the Installation Wizard displays. Click **Next** to begin the installation process.

CipherTrust
ENTERPRISE EMAIL SECURITY
IronMail™
CipherTrust Installation Wizard
This wizard will take you step-by-step through the network configuration of the IronMail.. Once you have entered all the information, the system will reboot and the Web Administration will be accessible.
Next

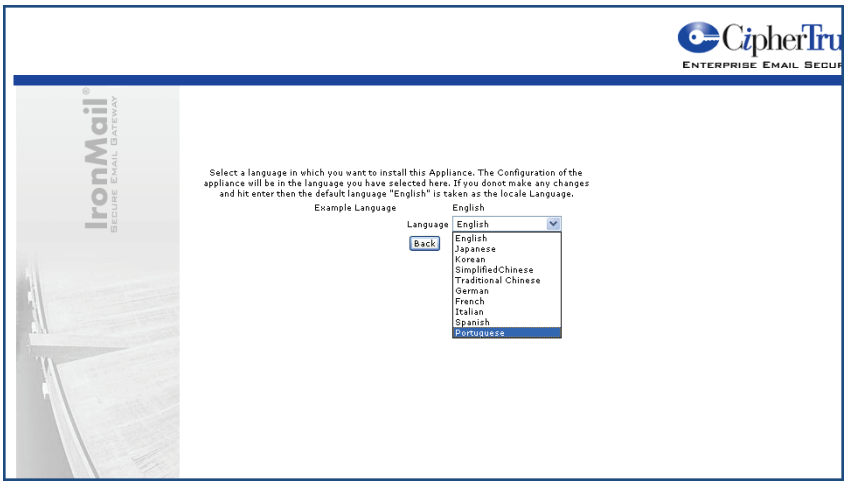
2. The first screen to appear is the Master Sale and License Agreement. After you have read the agreement, click **Accept** or **Decline**. If you choose to Decline, the installation wizard will close and the appliance will not run. If you choose Accept, the wizard proceeds to the next step.


IronMail™
CipherTrust Installation Wizard
MASTER SALE AND LICENSE AGREEMENT FOR THE
CIPHERTRUST® IRONMAIL® APPLIANCE
IMPORTANT: THIS MASTER SALE AND LICENSE AGREEMENT GOVERNS USE OF THE IRONMAIL® SOFTWARE AND, IF LICENSED IN ADDITION TO THE IRONMAIL® SOFTWARE, THE ANTI-VIRUS SOFTWARE (THE IRONMAIL® SOFTWARE AND, IF APPLICABLE, THE ANTI-VIRUS SOFTWARE COLLECTIVELY REFERRED TO AS THE "SOFTWARE") ON THE APPLIANCE HARDWARE ON WHICH THE SOFTWARE IS INSTALLED AND OPERATES (THE IRONMAIL® SOFTWARE AND APPLIANCE HARDWARE BEING REFERRED TO HEREIN TOGETHER AS THE "APPLIANCE"). READ THIS MASTER SALE AND LICENSE AGREEMENT CAREFULLY PRIOR TO USING THE APPLIANCE. IN ORDER TO USE THIS APPLIANCE, YOU MUST INDICATE ACCEPTANCE BY YOU AND BY THE CORPORATE OR BUSINESS ENTITY WHICH IS USING THE APPLIANCE ("CUSTOMER") TO THESE TERMS AND CONDITIONS BY CLICKING ON THE "Accept" BUTTON ON YOUR SCREEN. BY INDICATING YOUR AGREEMENT, YOU ALSO REPRESENT AND WARRANT THAT YOU ARE A DULY AUTHORIZED REPRESENTATIVE OF THE CUSTOMER AND THAT YOU HAVE THE RIGHT AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON ITS BEHALF. BY USING THE APPLIANCE, CUSTOMER EXPRESSLY AGREES WITH CIPHERTRUST, INC., A GEORGIA CORPORATION ("CIPHERTRUST"), TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE WITH ANY OF THE TERMS OR CONDITIONS OF THIS AGREEMENT, CUSTOMER IS NOT AUTHORIZED TO USE THE APPLIANCE FOR ANY PURPOSE WHATSOEVER; PLEASE IMMEDIATELY CEASE USE AND CONTACT CIPHERTRUST. Please print a copy of this Agreement for Customer's records.
1. License. This Agreement grants Customer (i) a non-exclusive, non-transferable license to use one copy of the IronMail® Software (the "IronMail® License"), and, if purchased by Customer, (ii) a non-exclusive, non-transferable license to use one copy of the anti-virus software for a specific period of time as indicated on the Customer's purchase order and/or CipherTrust's invoice (the "Anti-Virus License") (the IronMail® License and, if applicable, Anti-Virus License collectively referred to as the "License") solely on and in conjunction with the Appliance Hardware on which it is installed. This Agreement also authorizes Customer to use the related written materials and "online" or electronic documentation (collectively, "Documentation") solely in conjunction with the Appliance. CipherTrust and its suppliers retain title to all patents, copyrights, trade secrets, trademarks and other intellectual property rights in the Software and the Documentation. This Agreement shall not affect a sale of the Software, and Customer shall not acquire hereunder any right, title, or interest in the Software or Documentation, except the right to use them in accordance with this Agreement.
Customer from its possession and use of the Appliance during the Evaluation shall be treated as confidential per the terms of Section 14 herein. Upon Customer's payment for the Appliance and the license fee for the Software, the temporary License granted per this Section shall automatically become perpetual (subject to Section 2 herein). In the event Customer decides not to purchase the Appliance and a license for the Software, the temporary License granted per this Section will be automatically revoked at the end of the Evaluation Period, and Customer at its expense shall promptly return the Appliance to CipherTrust, properly packaged for commercial shipment to ensure no physical damage during transit; Customer will be invoiced by CipherTrust for an amount equal to the replacement cost of the Appliance should the returned Appliance be delivered to CipherTrust damaged due to insufficient and improper packaging by Customer. Upon Customer's failure to timely return the Appliance per the foregoing sentence, CipherTrust shall issue an invoice to Customer for the purchase at list price of the Appliance and a Software license under the terms of this Agreement. The terms of this Section shall apply only (i) to Customer's use and possession of the Appliance for Evaluation purposes and (ii) in the absence of a written evaluation agreement signed by both parties, which if executed shall prevail and control during the Evaluation Period. The terms stated in Sections 2, 5 and 16 of this Agreement shall not apply during the Evaluation Period.
18. General. This Agreement is the complete and exclusive statement of the agreement between Customer and CipherTrust concerning the subject matter covered hereby, this Agreement supersedes any prior proposal, agreement, or communication, oral or written, pertaining to the such subject matter and there are no inducements to enter into this Agreement which are not set forth herein. All products and services provided hereunder are provided per the terms and conditions stated in this Agreement, which supersede any different terms and conditions contained in Customer's purchase order(s) or any other Customer document that may be accepted by CipherTrust for Customer's convenience; CipherTrust hereby objects to the terms and conditions of such Customer documents to the extent they conflict herewith. This Agreement shall be governed by the laws of the State of Georgia and of the United States of America, excluding (i) their respective conflicts of law principles and (ii) the United Nations Convention on Contracts for the International Sale of Goods.
Do you agree to the terms and conditions set forth in this Master Sale and License Agreement?
Accept
Decline

3. The next screen that opens displays the Support Services Agreement. After you have read the agreement, click **Accept** or **Decline**. If you choose to Decline, the installation wizard will close and the appliance will not run. If you choose Accept, the wizard proceeds to the next step.


IronMail™
CipherTrust Installation Wizard
SUPPORT SERVICES AGREEMENT FOR THE
CIPHERTRUST® IRONMAIL® APPLIANCE
IMPORTANT: THIS SUPPORT SERVICES AGREEMENT GOVERNS THE ANNUAL MAINTENANCE AND SUPPORT SERVICES PROVIDED BY CIPHERTRUST, INC., A GEORGIA CORPORATION ("CIPHERTRUST") AND ITS AUTHORIZED AGENTS TO CUSTOMER FOR THE IRONMAIL® SOFTWARE AND, IF SO LICENSED BY CUSTOMER, ANTI-VIRUS SOFTWARE LICENSED DIRECTLY FROM CIPHERTRUST (THE IRONMAIL® SOFTWARE AND ANY ANTI-VIRUS SOFTWARE COLLECTIVELY REFERRED TO HEREIN AS THE "SOFTWARE") AND FOR THE COMPUTER HARDWARE ("APPLIANCE HARDWARE") ON WHICH SUCH SOFTWARE IS INSTALLED AND OPERATES (THE IRONMAIL® SOFTWARE AND APPLIANCE HARDWARE COLLECTIVELY REFERRED TO HEREIN AS THE "APPLIANCE"), AND, IF REQUESTED AND PAID FOR BY CUSTOMER, INSTALLATION, INTEGRATION AND TRAINING SERVICES RELATED TO THE APPLIANCE. READ THIS SUPPORT SERVICES AGREEMENT CAREFULLY PRIOR TO USING THE APPLIANCE. IN ORDER TO RECEIVE SUPPORT SERVICES FOR THE APPLIANCE, YOU MUST INDICATE ACCEPTANCE BY YOU AND BY THE CORPORATE OR BUSINESS ENTITY USING THE APPLIANCE ("CUSTOMER") TO THESE TERMS AND CONDITIONS BY CLICKING ON THE "Accept" BUTTON ON YOUR SCREEN. BY INDICATING YOUR AGREEMENT, YOU ALSO REPRESENT AND WARRANT THAT YOU ARE A DULY AUTHORIZED REPRESENTATIVE OF THE CUSTOMER AND THAT YOU HAVE THE RIGHT AND AUTHORITY TO ENTER INTO THIS AGREEMENT ON ITS BEHALF. BY USING THE APPLIANCE AND BY REQUESTING AND RECEIVING SUPPORT SERVICES FOR THE APPLIANCE, CUSTOMER EXPRESSLY AGREES WITH CIPHERTRUST TO BE BOUND BY ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF CUSTOMER DOES NOT AGREE WITH ANY OF THE TERMS OR CONDITIONS OF THIS AGREEMENT, CUSTOMER IS NOT AUTHORIZED TO REQUEST OR RECEIVE SUPPORT SERVICES FOR THE APPLIANCE; PLEASE IMMEDIATELY CEASE USE OF CIPHERTRUST SUPPORT SERVICES AND CONTACT CIPHERTRUST IMMEDIATELY.
Please print a copy of this Agreement for Customer's records.
1. Support Services. CipherTrust shall provide Customer telephone technical consultation, Updates (as defined herein) and Error correction (as defined herein) as software maintenance and support services related to the Software ("Software Support") and telephone technical consultation and onsite hardware repair services as maintenance and support services related to the Appliance Hardware ("Appliance Hardware Support") during periods of contracted Support (the Software Support and Appliance Hardware Support hereinafter referred to together as the "Support Services" or "Support").
6. Notice; Dispute Resolution. Any notices to be given under this Agreement shall be (i) sent to the address of the party's United States corporate headquarters, to the attention of its CEO and copied to its Legal Counsel, (ii) delivered by hand, via US Mail (postage prepaid, certified or registered), or via a document delivery service, and (iii) deemed given upon receipt. All disputes arising out of or relating to this Agreement shall be finally settled by arbitration conducted in Atlanta, Georgia, United States under the Rules of Commercial Arbitration of the American Arbitration Association. The parties shall bear equally the cost of the arbitration (exclusive of legal fees and expenses, all of which each party shall bear separately). All decisions of the arbitrator(s) shall be final and binding on both parties and enforceable in any court of competent jurisdiction. Notwithstanding the foregoing, in the event of breach by a party of its obligations hereunder, the non-breaching party may seek injunctive or other equitable relief in any court of competent jurisdiction, without necessity of posting bond. Customer acknowledges that infringement of intellectual property of CipherTrust or unauthorized copying would cause irreparable harm to CipherTrust.
7. General. This Agreement is the complete and exclusive statement of the agreement between Customer and CipherTrust pertaining to the subject matter of this Agreement, and this Agreement supersedes any prior proposal, agreement, or communication, oral or written, pertaining thereto and there are no inducements to enter into this Agreement which are not set forth herein. All Support and other services provided hereunder are provided per the terms and conditions stated in this Agreement, which supersede any different terms and conditions contained in Customer's purchase order(s) or any other Customer document that may be accepted by CipherTrust for Customer's convenience; CipherTrust hereby objects to the terms and conditions of such Customer documents to the extent they conflict herewith. This Agreement shall be governed by the laws of the State of Georgia and of the United States of America, excluding (i) their respective conflicts of law principles and (ii) the United Nations Convention on Contracts for the International Sale of Goods.
Do you agree to the terms and conditions set forth in this Support Services Agreement?
Accept
Decline

4. Select the language you wish to use for this installation of IronMail by choosing the name of the language from the pick list.



Click Next.

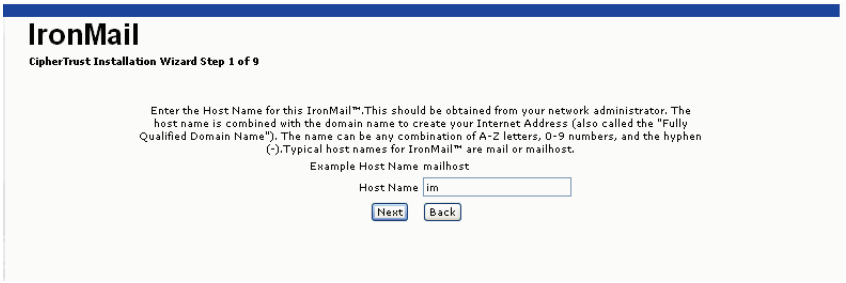
5. Copy the text file containing the License Key for the appliance, and paste the key into the input field on the next screen.

   You must include all of the beginning and ending lines that appear with the License Key, as shown:

   "======Begin CipherTrust License======" and "======End CipherTrust License======."

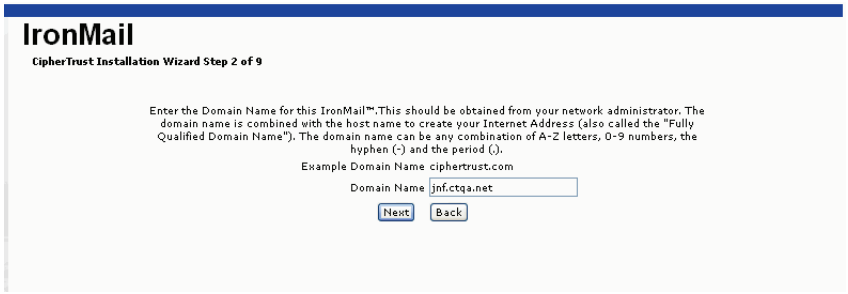
   After pasting in the key, click **Next**.

6. Enter the host name for the appliance, created by your Network Administrator. The host name is the text preceding the domain name. In the example "servername.yourdomain.com" "servername" is the host name, and "yourdomain.com" is the domain name.


IronMail
CipherTrust Installation Wizard Step 1 of 9
Enter the Host Name for this IronMail™.This should be obtained from your network administrator. The host name is combined with the domain name to create your Internet Address (also called the "Fully Qualified Domain Name"). The name can be any combination of A-Z letters, 0-9 numbers, and the hyphen (-).Typical host names for IronMail™ are mail or mailhost.
Example Host Name mailhost
Host Name im
Next
Back

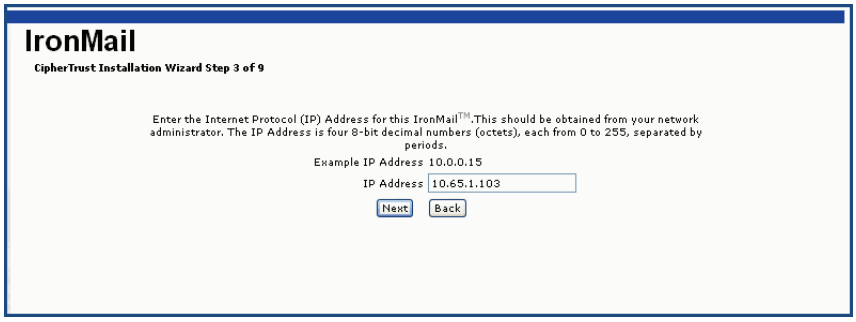
   Click **Next**.

7. Enter the domain name for the domain to which the appliance will belong (e.g., "yourdomain.com").


IronMail
CipherTrust Installation Wizard Step 2 of 9
Enter the Domain Name for this IronMail™.This should be obtained from your network administrator. The domain name is combined with the host name to create your Internet Address (also called the "Fully Qualified Domain Name"). The domain name can be any combination of A-Z letters, 0-9 numbers, the hyphen (-) and the period (.).
Example Domain Name ciphertrust.com
Domain Name jnf.ctqa.net
Next
Back

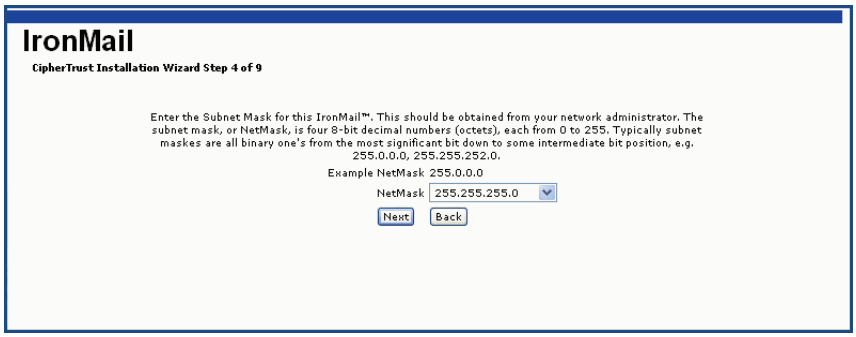
Click **Next**.

8. Enter the IP address assigned by your Network Administrator for this appliance.


IronMail
CipherTrust Installation Wizard Step 3 of 9
Enter the Internet Protocol (IP) Address for this IronMail™.This should be obtained from your network administrator. The IP Address is four 8-bit decimal numbers (octets), each from 0 to 255, separated by periods.
Example IP Address 10.0.0.15
IP Address 10.65.1.103
Next
Back

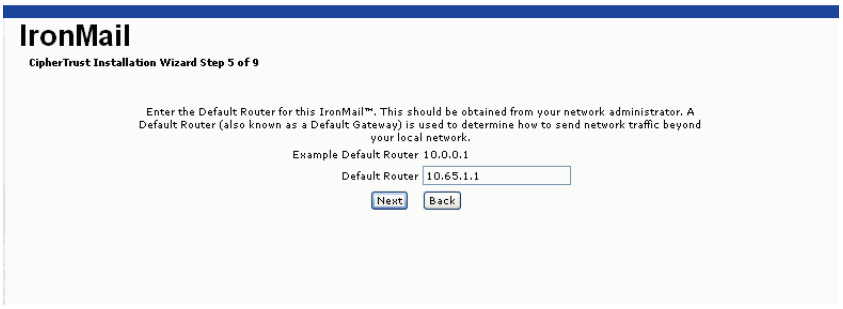
Click **Next**.

9. Enter the subnet mask for this IronMail, as provided by your Network Administrator.


IronMail
CipherTrust Installation Wizard Step 4 of 9
Enter the Subnet Mask for this IronMail™. This should be obtained from your network administrator. The subnet mask, or NetMask, is four 8-bit decimal numbers (octets), each from 0 to 255. Typically subnet maskes are all binary one's from the most significant bit down to some intermediate bit position, e.g. 255.0.0.0, 255.255.252.0.
Example NetMask 255.0.0.0
NetMask 255.255.255.0
Next
Back

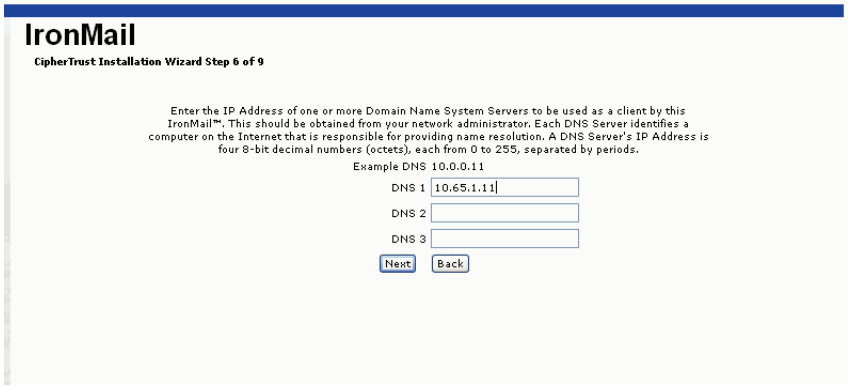
Click **Next**.

10. Enter the IP address for the Default Router for this appliance. The router address is provided by the Network Administrator.


IronMail
CipherTrust Installation Wizard Step 5 of 9
Enter the Default Router for this IronMail™. This should be obtained from your network administrator. A Default Router (also known as a Default Gateway) is used to determine how to send network traffic beyond your local network.
Example Default Router 10.0.0.1
Default Router 10.65.1.1
Next
Back

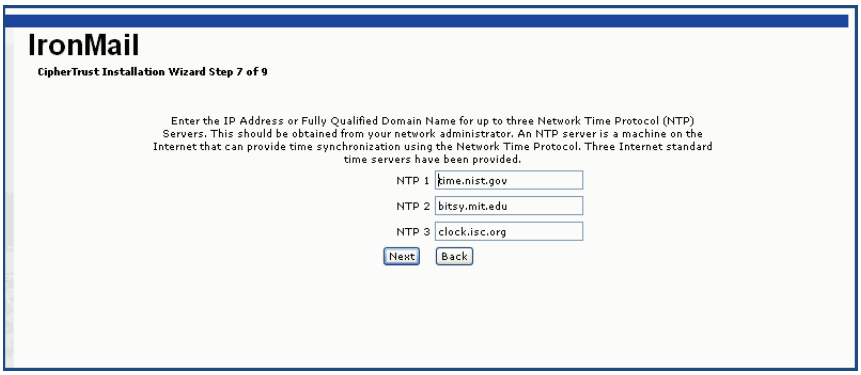
Click **Next**.

11. Enter the IP address for at least one of your DNS Servers (you may have up to three). The DNS server will be used as a client for this IronMail.


IronMail
CipherTrust Installation Wizard Step 6 of 9
Enter the IP Address of one or more Domain Name System Servers to be used as a client by this IronMail™. This should be obtained from your network administrator. Each DNS Server identifies a computer on the Internet that is responsible for providing name resolution. A DNS Server's IP Address is four 8-bit decimal numbers (octets), each from 0 to 255, separated by periods.
Example DNS 10.0.0.11
DNS 1 10.65.1.11
DNS 2
DNS 3
Next
Back

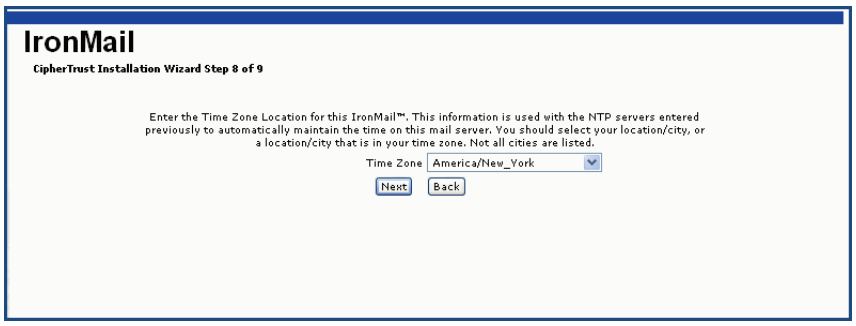
Click **Next**.

12. Enter the IP address or the fully qualified domain name for up to three Network Time Protocol (NTP) servers, as provided by the Network Administrator.


IronMail
CipherTrust Installation Wizard Step 7 of 9
Enter the IP Address or Fully Qualified Domain Name for up to three Network Time Protocol (NTP) Servers. This should be obtained from your network administrator. An NTP server is a machine on the Internet that can provide time synchronization using the Network Time Protocol. Three Internet standard time servers have been provided.
NTP 1 time.nist.gov
NTP 2 bitsy.mit.edu
NTP 3 clock.isc.org
Next
Back

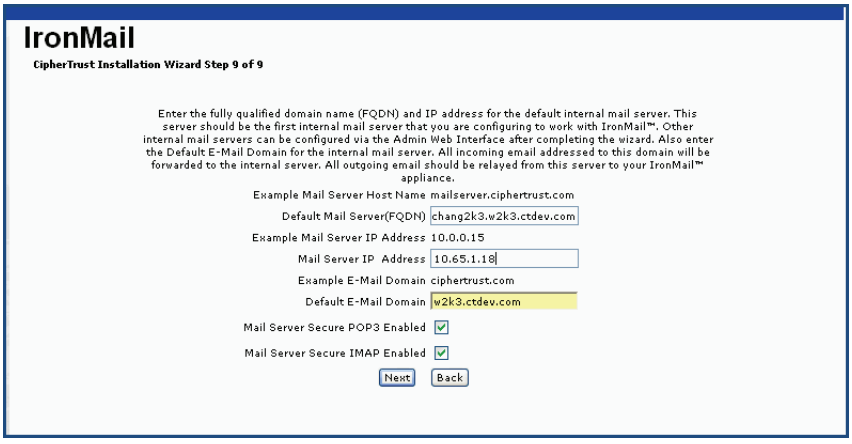
Click **Next**.

13. Specify the appliance's time zone by selecting from the pick list your own location or city, or a location/city that is in the same time zone.


IronMail
CipherTrust Installation Wizard Step 8 of 9
Enter the Time Zone Location for this IronMail™. This information is used with the NTP servers entered previously to automatically maintain the time on this mail server. You should select your location/city, or a location/city that is in your time zone. Not all cities are listed.
Time Zone
America/New_York
Next
Back

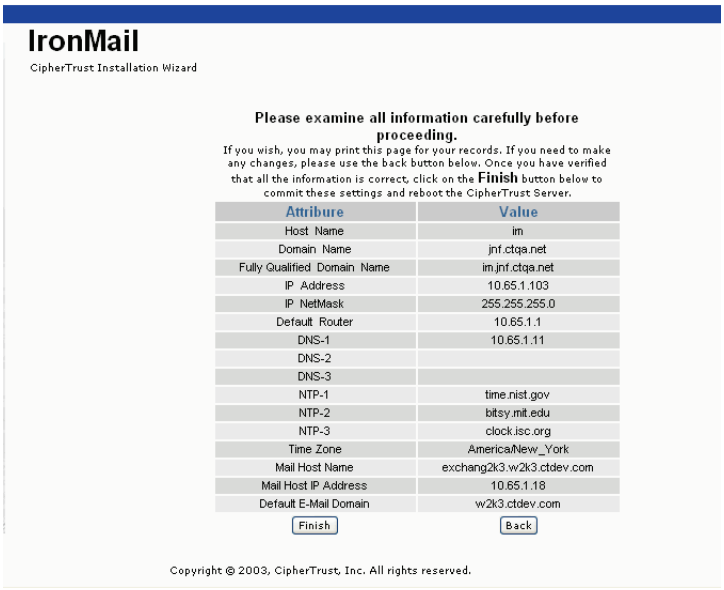
Click **Next**.

14. If you are configuring ***a stand-alone IronMail appliance***, you must enter information about your default email server. If you have more than one email server, enter only the information about the default server. You can configure additional servers after you complete the Installation Wizard.


IronMail
CipherTrust Installation Wizard Step 9 of 9
Enter the fully qualified domain name (FQDN) and IP address for the default internal mail server. This server should be the first internal mail server that you are configuring to work with IronMail™. Other internal mail servers can be configured via the Admin Web Interface after completing the wizard. Also enter the Default E-Mail Domain for the internal mail server. All incoming email addressed to this domain will be forwarded to the internal server. All outgoing email should be relayed from this server to your IronMail™ appliance.
Example Mail Server Host Name mailserver.ciphertrust.com
Default Mail Server(FQDN) chang2k3.w2k3.ctdev.com
Example Mail Server IP Address 10.0.0.15
Mail Server IP Address 10.65.1.18
Example E-Mail Domain ciphertrust.com
Default E-Mail Domain w2k3.ctdev.com
Mail Server Secure POP3 Enabled
Mail Server Secure IMAP Enabled
Next
Back

If you are configuring a Centralized Management Console, you do not have to provide information about internal mail servers. Skip this step by clicking **Next**, and proceed to verifying your information.

15. Verify that the information you have provided is correct. You can use the Back buttons to return to previous steps and make corrections, should you detect errors. You may want to print this screen for your records once you have verified the information.

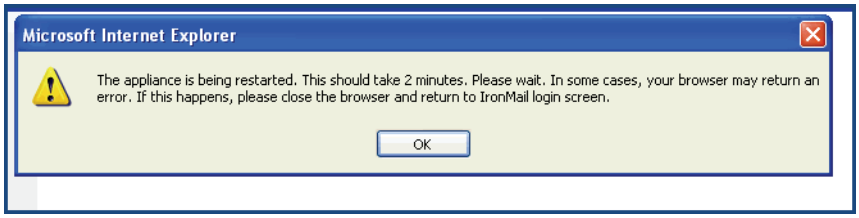


If you inadvertently enter the IP address incorrectly and fail to print this page showing the appliance's dot-decimal number, you will be unable to log onto IronMail when you later browse to what you thought was the correct address. Log onto IronMail via attached keyboard and command line interface to reset the appliance to its default factory settings.

Click **Finish** after the information has been verified.

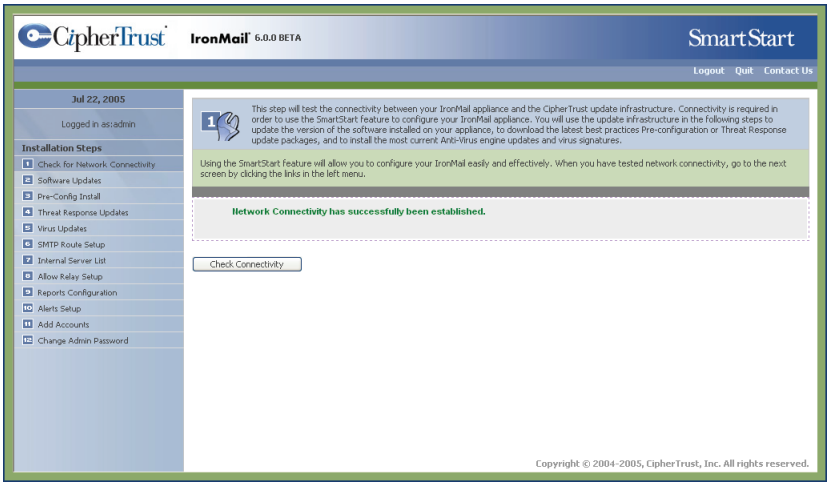
CAUTION: Do not press Enter a second time or click the Refresh icon. This can cause problems with program integrity.

IronMail will automatically restart. The following message will display.


Microsoft Internet Explorer
The appliance is being restarted. This should take 2 minutes. Please wait. In some cases, your browser may return an error. If this happens, please close the browser and return to IronMail login screen.
OK

When the restart process has had time to finish (wait at least three minutes), you may log onto the appliance. Using your network browser, go to the IP address for the appliance and log in.

IronMail's opening SmartStart screen will display, allowing you to continue with “best practices” configuration.


CipherTrust
IronMail 6.0.0 BETA
SmartStart
Logout
Quit
Contact Us
Jul 22, 2005
Logged in as:admin
Installation Steps
1 Check for Network Connectivity
2 Software Updates
3 Pre-Config Install
4 Threat Response Updates
5 Virus Updates
6 SMTP Route Setup
7 Internal Server List
8 Allow Relay Setup
9 Reports Configuration
10 Alerts Setup
11 Add Accounts
12 Change Admin Password
This step will test the connectivity between your IronMail appliance and the CipherTrust update infrastructure. Connectivity is required in order to use the SmartStart feature to configure your IronMail appliance. You will use the update infrastructure in the following steps to update the version of the software installed on your appliance, to download the latest best practices Pre-configuration or Threat Response update packages, and to install the most current Anti-Virus engine updates and virus signatures.
Using the SmartStart feature will allow you to configure your IronMail easily and effectively. When you have tested network connectivity, go to the next screen by clicking the links in the left menu.
Network Connectivity has successfully been established.
Check Connectivity
Copyright © 2004-2005, CipherTrust, Inc. All rights reserved.

Once a stand-alone IronMail is running, it is now acting as a proxy—incoming and outgoing mail will flow through IronMail to the email server you specified, and your exposure to the outside world has been "hardened.” However, many of IronMail’s features have not yet been enabled. Additional configuration is required as described in the remainder of the *User Manual*.

Network Connectivity

DNS Configuration

Domain Name Service (DNS) is an exceedingly complex subject, and there is no standard way in which it is implemented. In simple terms, DNS allows multiple servers to appear as if the have the same host name. In addition to the DNS server's MX, A, PTR and other records, some networks use Network Address Tables (NAT) to map servers internally. However you implement DNS, you must at least do the following:

- You must create MX, A and PTR records for the IronMail appliance, and
- You must give IronMail a lower preference number than your mail server's MX record.

This will allow all mail addressed to your domain to be routed to the IronMail appliance, and allow all other servers to perform DNS lookups and reverse lookups on IronMail. The Administrator or Installer names the DNS Server during the initial configuration of IronMail. The preference or priority is set after the initial setup, as a System function for configuring IronMail.

The most common use of DNS is to perform "forward lookup" (resolving a fully qualified domain name, such as "servername.yourdomain.com," with a valid IP address such as 63.168.166.231). DNS is also capable of "reverse lookup" (resolving an IP address to a fully qualified domain name). The reverse lookup may also be used to detect (and reject) certain kinds of "address spoofing" used by hackers. Most Internet email servers use both of these features.

For a reverse lookup to work, you must publish a reverse zone (e.g., 166.168.63.in-addr.arpa) that contains PTR records mapping IP addresses onto node names. You must create a reverse zone, with your IP address in reverse octet order, followed by the text string "in-addr.arpa." For example, the forward zone is "yourdomain.com" and the reverse zone is "166.168.63.in-addr.arpa."

You can check whether reverse lookup is working using the "nslookup" command. Using nslookup on an IP address with that switch (in-addr.arpa) will do a reverse lookup (IP-to-Host Name), and display the resolved name, as shown below:

```
su-2.04# nslookup 10.0.3.101
Server:  pridocon.ctqa.net
Address:  10.0.3.55
Name:    im.ex.ctqa.net
Address:  10.0.3.101
```

An example of a forward lookup (Host-Name-to-IP) follows:

```
su-2.04# nslookup im.ex.ctqa.net
Server:  pridocon.ctqa.net
Address:  10.0.3.55
Name:    im.ex.ctqa.net
Address:  10.0.3.101
```

Internal Mail Server Configuration

Configuration of your internal mail servers is very simple. Make IronMail the only IP address allowed to connect to your mail server, and re-direct your servers' outbound mail flow to IronMail using a static route.

Network Firewall Configuration

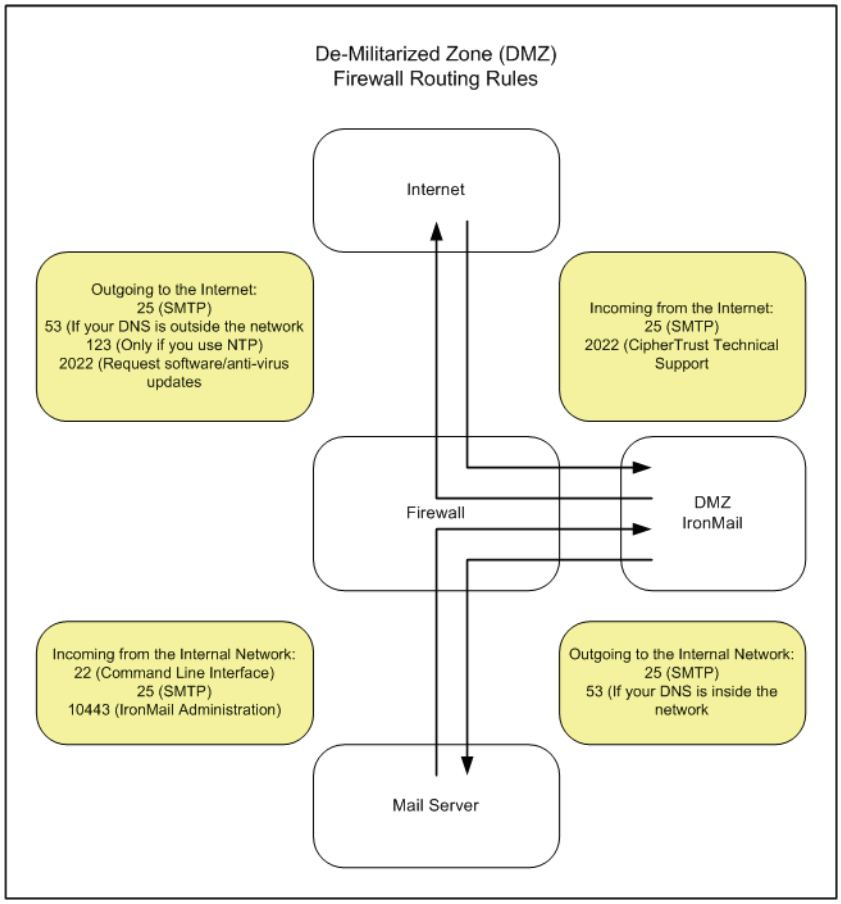
Your network administrator must assign an IP address, subnet mask, and host name for the IronMail appliance. (A host name "yourname" and domain name "yourdomain.com" results in the fully qualified domain name (FQDN) "yourname.yourdomain.com.") The first time you connect to IronMail, you will be required to enter this and other information into its installation wizard. Establishing network connectivity may require the assistance of your network administrator.

Based on your company's network design, IronMail may be connected to the corporate network either in a De-Militarized Zone (DMZ) or on the internal LAN. Once the physical connection has been established, some configuration of the network firewall and Domain Name Service (DNS) will be required.

Configuring the Firewall

There are three main styles of firewalls: packet filter-types (routers with ACLs), application proxy-types (e.g., Raptor and TIS Gauntlet), and stateful inspection-types (e.g., CheckPoint and Cisco PIX). It is important to understand most application proxy firewalls do not support SMTP over SSL (i.e. the SMTPS protocol). If your firewall is an application proxy-type that does not support SSL, IronMail will not be able to encrypt your mail. Both packet filter and stateful inspection firewalls, however, fully support SMTP over SSL if they are configured correctly.

It is recommended that you place IronMail in a DMZ if your network supports it. If you do so, you must create rules to allow the protocols for "outside world to IronMail," "IronMail to outside world," "IronMail to the internal mail server," and "internal mail server to IronMail." There should be no open protocols from outside to inside (bypassing IronMail) when using a DMZ configuration. The following diagram and table describe the ports you must open in your firewall to allow IronMail to function correctly:



A key advantage to the DMZ configuration is that IronMail's analysis of incoming messages is performed before the messages actually penetrate the firewall. IronMail sends its output back to the firewall before it is allowed inside the system. With a non-DMZ placement, incoming messages are inside the firewall before IronMail scans them.

Outgoing to the Internet: Rules to allow Edge to open a connection to the Internet

Port	TCP/UDP	Protocol	Description
Port 25	TCP	SMTP	Required for mail reception
Port 123	TCP/UDP	NTP	Required if using Network Time Protocol
Port 53	TCP/UDP	DNS	Optional for an IronMail/CMC (if your DNS is outside the network, you must open the port allowing IronMail/CMC to connect to it).
Port 20022	TCP	Cipher-Trust	Required in order for IronMail to request software/anti-virus updates

Incoming from the Internet: Rules to allow IronMail to accept connections from the Internet

Port	TCP/UDP	Protocol	Description
Port 25	TCP	SMTP	Required for mail reception
Port 20022	TCP	Cipher-Trust	Optional (allows CipherTrust to connect to your IronMail for Technical Support)

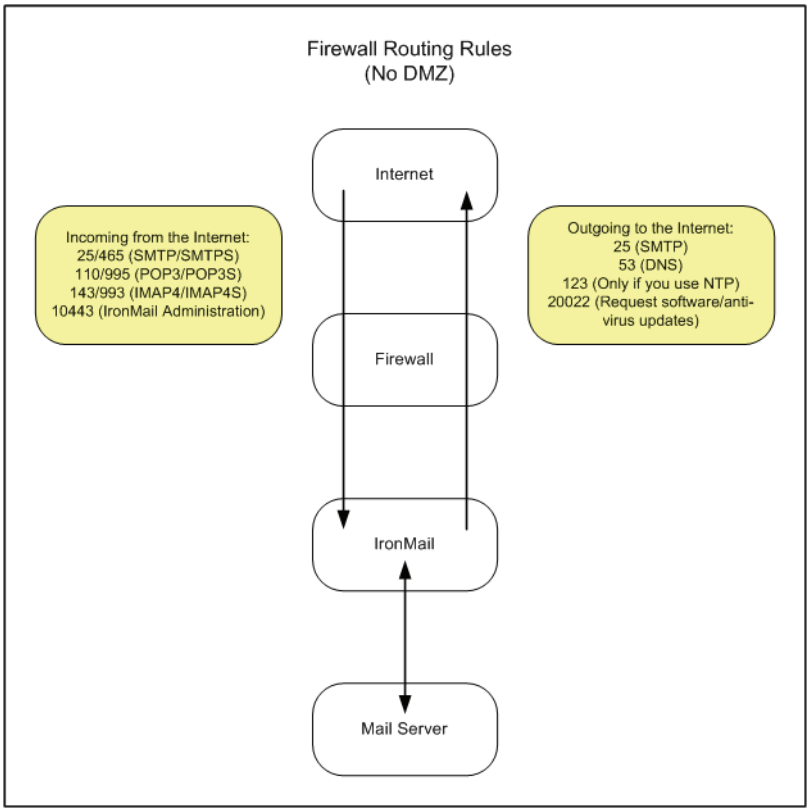
Outgoing to the Internal Network: Rules that allow IronMail to connect to the mail servers

Port	TCP/UDP	Protocol	Description
Port 25	TCP	SMTP	Required for mail delivery
Port 53	TCP/UDP	DNS	Optional for an IronMail/CMC (if your DNS is outside the network, you must open the port allowing IronMail/CMC to connect to it).

Incoming from the Internal Network: Rules to allow IronMail to receive connections from the mail servers.

Port	TCP/UDP	Protocol	Description
Port 22	TCP	Command Line Interface	Optional (only if you want to access the command line interface from inside the network)
Port 25	TCP	SMTP	Required for mail delivery
Port 10443	TCP	HTTPS	Required (this is the port used to connect to IronMail's WebAdmin interface)

If you do not have a DMZ, it is safe to install the IronMail appliance on your internal network because its hardened face and built-in firewall features protect it. If you install IronMail inside the network, simply open the necessary "port holes" in the firewall. Ensure that your firewall's port settings match the previous table.



Most mail servers use only ports 25, 110, and 143 for sending and retrieving email. However, email transmitted through these ports is unsecured—attackers can read or intercept email sent this way. We recommend that you open the secure ports instead: 995 for POP3S and 993 for IMAP4S to force external users to retrieve their mail via SSL. (IronMail provides the ability to send mail securely on port 25.)

IronMail has a standard configuration for Maximum Transmission Unit (the maximum size for a single packet that may be transferred by the email system) of 1,500 bytes. If your system requires a maximum other than the standard MTU configuration, a custom configuration can be accomplished by CipherTrust's Customer Service group.

Best Practices Configuration

The concept of "Best Practices" configuration is derived from CipherTrust's desire to streamline the process of preparing the IronMail appliance for effective operation. SmartStart offers the means to do precisely that.

In this chapter

In this chapter, you will find information about the following topics:

- SmartStart
  - Using SmartStart

SmartStart

The purpose for SmartStart is to provide the Administrator the ability to install best practices IronMail configurations at the time of initial appliance installation and setup. It allows the Administrator to install the current software upgrades, current Anti-Virus upgrades, the Pre-Configuration package, the current Threat Response Update (TRU), and several other common configuration entries.

The Administrator will complete the initial IronMail setup and installation as usual, applying the standard Installation Wizard, as explained in the previous chapter and in the *IronMail Setup Guide*. Then, at the Administrator's first login, the initial SmartStart screen displays.

Unless the SmartStart installation is interrupted, subsequent logons will bypass SmartStart and take the user directly to the Dashboard, as discussed later in this manual.

Note: SmartStart functionality is available only to the Admin user account. For any other user, the first login will open the Dashboard, IronMail's regular opening screen.

Using SmartStart

Complete SmartStart installation requires completing the actions on 12 screens. It is important for the Administrator to remember a few basic rules for navigating SmartStart.

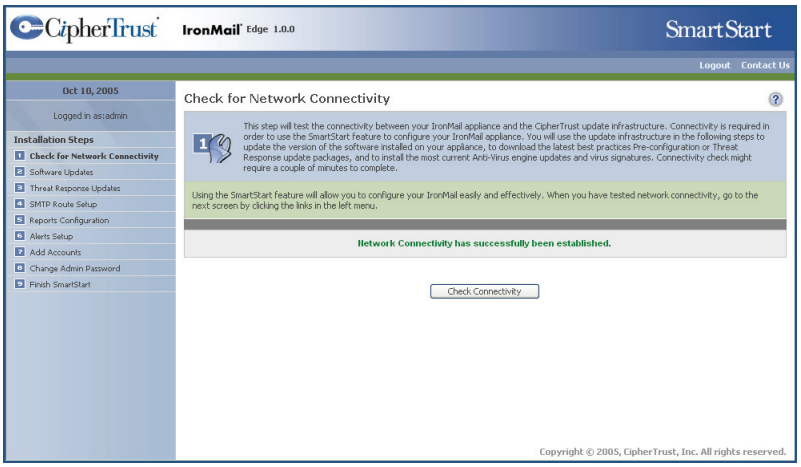
1. You must select the specific SmartStart screen you wish to use by clicking the screen's link in the left menu. When you finish one screen, you can go to the next by clicking its link.
2. If you need to leave the SmartStart Wizard before you have completed work with all screens, you must leave by clicking **Log Out**

at the top of the screen. The next time you log in, IronMail will return you to the SmartStart screen from which you logged out.

3. If you click **Quit** at the top of the screen, you will leave SmartStart, and will be taken to the Dashboard screen. You will not automatically return to SmartStart when you log in again.
4. Since some SmartStart steps need to be done in a specific order, please read the instructions on each screen before you apply it.

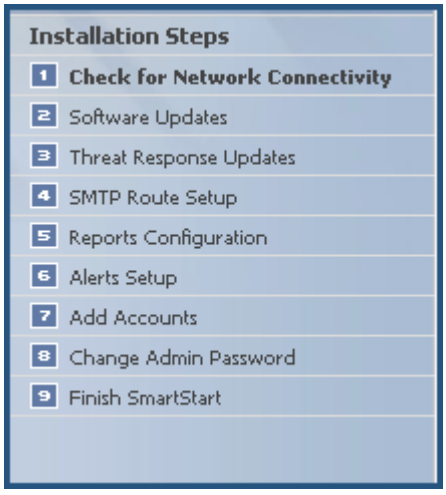
The SmartStart Screen

As illustrated in the screen shot that follow, SmartStart screens are divided into three sections.


CipherTrust
IronMail Edge 1.0.0
SmartStart
Logout Contact Us
Oct 10, 2005
Logged in as:admin
Installation Steps
1 Check for Network Connectivity
2 Software Updates
3 Threat Response Updates
4 SMTP Route Setup
5 Reports Configuration
6 Alerts Setup
7 Add Accounts
8 Change Admin Password
9 Finish SmartStart
Check for Network Connectivity
This step will test the connectivity between your IronMail appliance and the CipherTrust update infrastructure. Connectivity is required in order to use the SmartStart feature to configure your IronMail appliance. You will use the update infrastructure in the following steps to update the version of the software installed on your appliance, to download the latest best practices Pre-configuration or Threat Response update packages, and to install the most current Anti-Virus engine updates and virus signatures. Connectivity check might require a couple of minutes to complete.
Using the SmartStart feature will allow you to configure your IronMail easily and effectively. When you have tested network connectivity, go to the next screen by clicking the links in the left menu.
Network Connectivity has successfully been established.
Check Connectivity
Copyright © 2005, CipherTrust, Inc. All rights reserved.

Left Side: Menu

The left side of the screen contains the menu listing all 9 screens that may be used in SmartStart for IronMail Edge. You will use this menu to select the portion of the wizard you wish to apply.



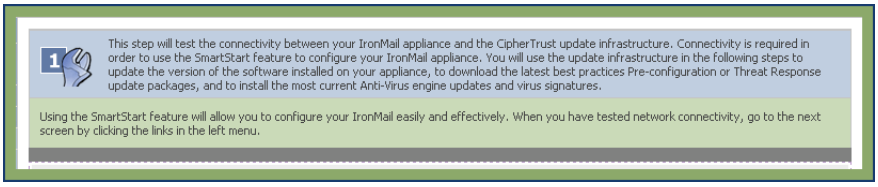
You may click on any SmartStart screen link to open it without regard for the order on the menu. However, some of the steps must be taken in order. Read the screen instructions before you apply the screen.

Screen 1, the Network Connectivity check, is the opening screen for SmartStart, since connectivity is required to apply some of the other steps.

Upper Right: SmartStart information

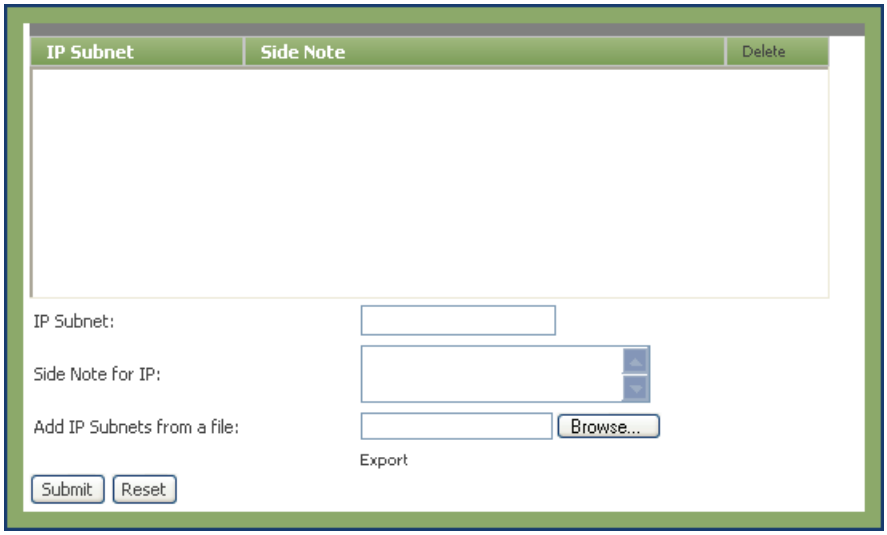
The upper portion of the screen, as seen below, extending across the screen except for the left menu area, contains informative text about

the screen you are currently viewing. It may provide instructions and other important information about the step you are about to complete.


This step will test the connectivity between your IronMail appliance and the CipherTrust update infrastructure. Connectivity is required in order to use the SmartStart feature to configure your IronMail appliance. You will use the update infrastructure in the following steps to update the version of the software installed on your appliance, to download the latest best practices Pre-configuration or Threat Response update packages, and to install the most current Anti-Virus engine updates and virus signatures.
Using the SmartStart feature will allow you to configure your IronMail easily and effectively. When you have tested network connectivity, go to the next screen by clicking the links in the left menu.

Lower Right: Configuration screens

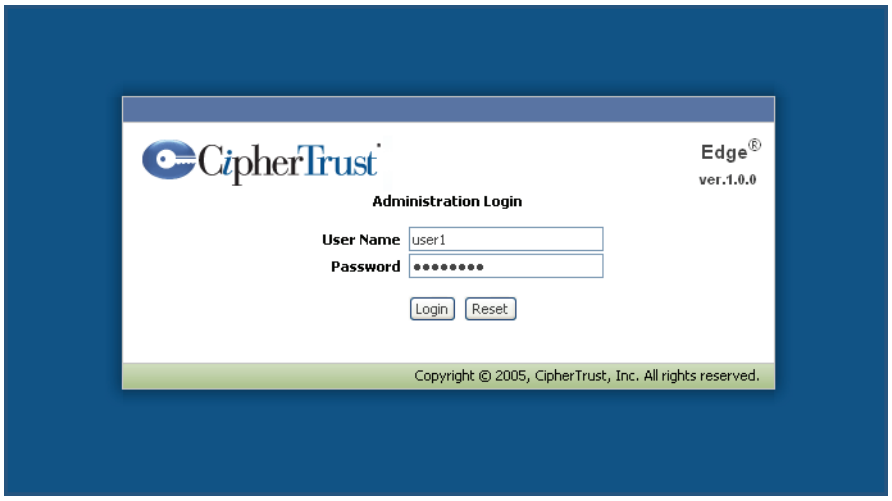
The lower portion of all SmartStart screens, like the sample below, will contain the actual IronMail configuration screens required to complete the specific step you are applying.



IMPORTANT: The screen images that populate this portion of the SmartStart screen will retain their own instruction text or help text.

Accessing SmartStart

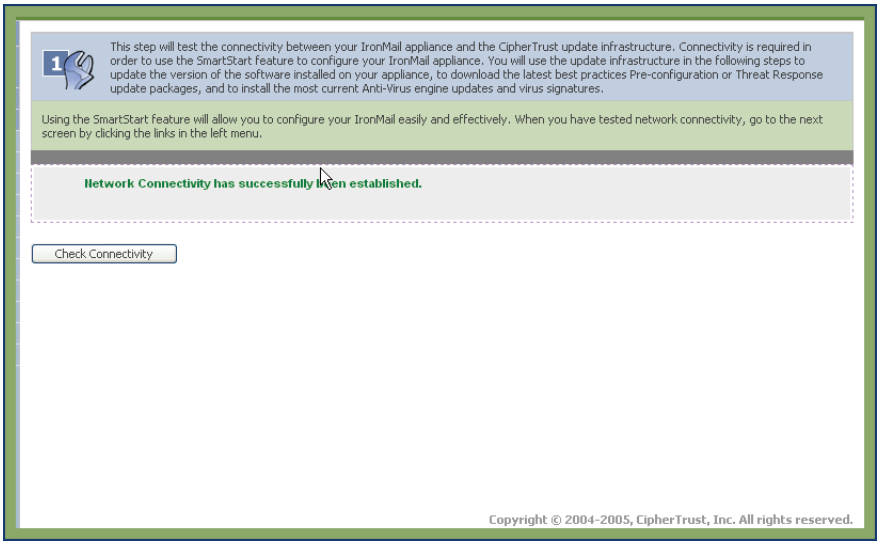
To access SmartStart as part of the initial installation and setup of the IronMail, the Administrator (Admin user account) simply logs into IronMail the first time.



Screen 1 of the SmartStart process opens.

Screen 1: Network Connectivity

The initial screen is designed to welcome the administrator, give basic SmartStart instruction, and test for Network Connectivity.


This step will test the connectivity between your IronMail appliance and the CipherTrust update infrastructure. Connectivity is required in order to use the SmartStart feature to configure your IronMail appliance. You will use the update infrastructure in the following steps to update the version of the software installed on your appliance, to download the latest best practices Pre-configuration or Threat Response update packages, and to install the most current Anti-Virus engine updates and virus signatures.
Using the SmartStart feature will allow you to configure your IronMail easily and effectively. When you have tested network connectivity, go to the next screen by clicking the links in the left menu.
Network Connectivity has successfully been established.
Check Connectivity
Copyright © 2004-2005, CipherTrust, Inc. All rights reserved.

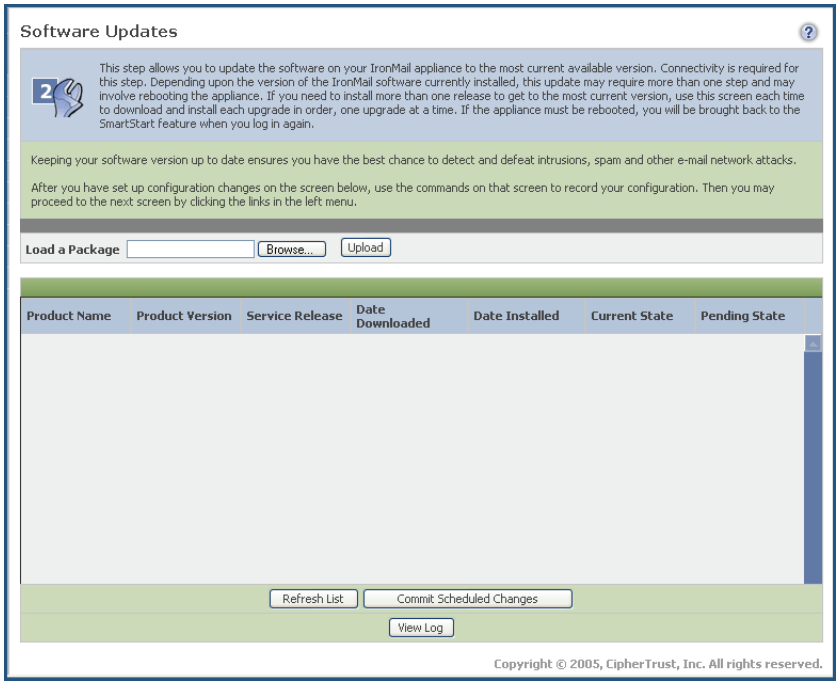
SmartStart Network Connectivity Check

This step tests the connectivity between your IronMail appliance and the CipherTrust update infrastructure. Connectivity is required in order to use the SmartStart feature for configuring your IronMail. You will use the update infrastructure in some of the following steps to update the version of software installed on your appliance, to download the latest “best practices” Pre-Configuration or Threat Response Update packages, and to install the most current Anti-Virus engine updates and virus signatures.

When you have tested your network connectivity, go to the next screen by clicking that screen's link in the left menu.

Screen 2: Software Updates

This step allows you to update the software on your IronMail appliance to the most current available version.


Software Updates
This step allows you to update the software on your IronMail appliance to the most current available version. Connectivity is required for this step. Depending upon the version of the IronMail software currently installed, this update may require more than one step and may involve rebooting the appliance. If you need to install more than one release to get to the most current version, use this screen each time to download and install each upgrade in order, one upgrade at a time. If the appliance must be rebooted, you will be brought back to the SmartStart feature when you log in again.
Keeping your software version up to date ensures you have the best chance to detect and defeat intrusions, spam and other e-mail network attacks.
After you have set up configuration changes on the screen below, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking the links in the left menu.
Load a Package
Browse...
Upload
Product Name
Product Version
Service Release
Date Downloaded
Date Installed
Current State
Pending State
Refresh List
Commit Scheduled Changes
View Log
Copyright © 2005, CipherTrust, Inc. All rights reserved.

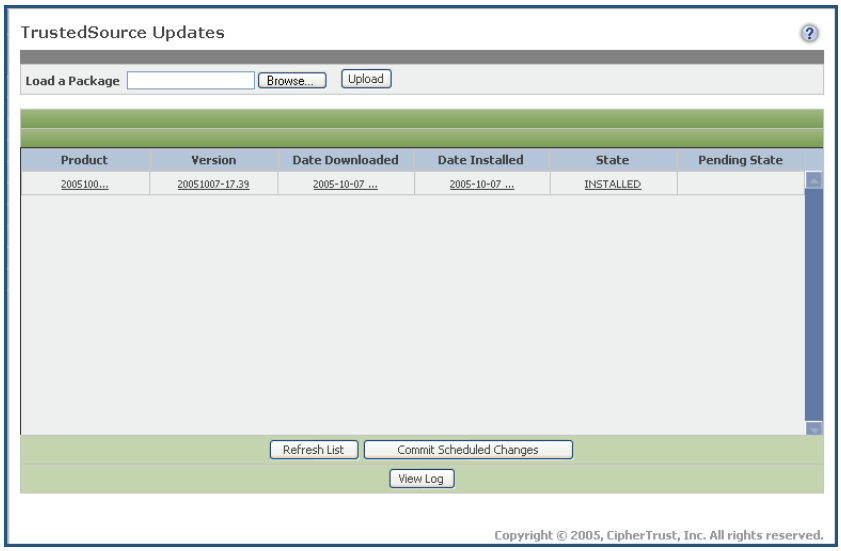
SmartStart Software Updates

Network connectivity is required for this step. Depending upon the version of the IronMail software currently installed, this update may require more than one step and may involve rebooting the appliance. If you need to install more than one release to get to the most current version, use this screen to download and install each upgrade in order, one upgrade at a time. If the appliance must be rebooted, you will be brought back to the SmartStart feature when you log in again.

After you have set up configuration changes on the screen shown at the bottom of the SmartStart page, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking that screen's link in the left menu.

Screen 3: TrustedSource Updates

For Edge, TRU updates take the form of TrustedSource updates. This screen allows you to access and install the latest TrustedSource Update package for your version of the IronMail Edge software.



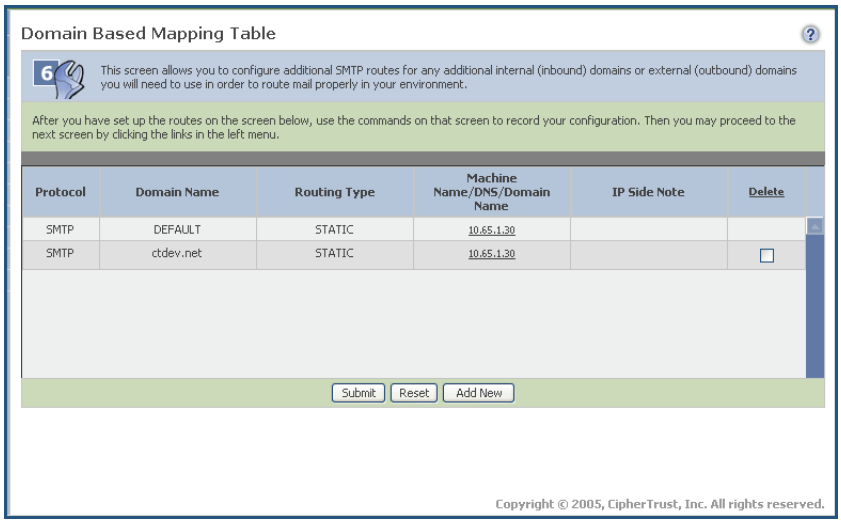
SmartStart TrustedSource Updates

IMPORTANT: You should install the TrustedSource package after upgrading to the most recent version of the IronMail Edge software.

After you have set up the installation on the screen at the bottom of the SmartStart page, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking that screen's link in the left menu.

Screen 4: SMTP Route Setup

This screen allows you to configure SMTP routes for any additional internal (inbound) domains or external (outbound) domains you will need in order to route mail properly in your environment.

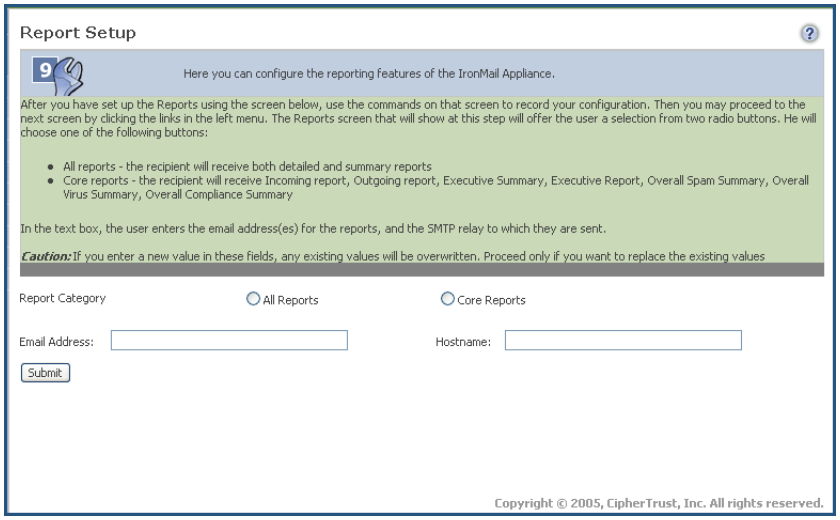

Domain Based Mapping Table
This screen allows you to configure additional SMTP routes for any additional internal (inbound) domains or external (outbound) domains you will need to use in order to route mail properly in your environment.
After you have set up the routes on the screen below, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking the links in the left menu.
Protocol
Domain Name
Routing Type
Machine Name/DNS/Domain Name
IP Side Note
Delete
SMTP
DEFAULT
STATIC
10.65.1.30
SMTP
ctdev.net
STATIC
10.65.1.30
Submit
Reset
Add New
Copyright © 2005, CipherTrust, Inc. All rights reserved.

SmartStart SMTP Route Setup

After you have set up the routes on the screen at the bottom of the SmartStart page, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking that screen's link in the left menu.

Screen 5: Report Setup

This screen allows you to configure the reporting features for your IronMail appliance.

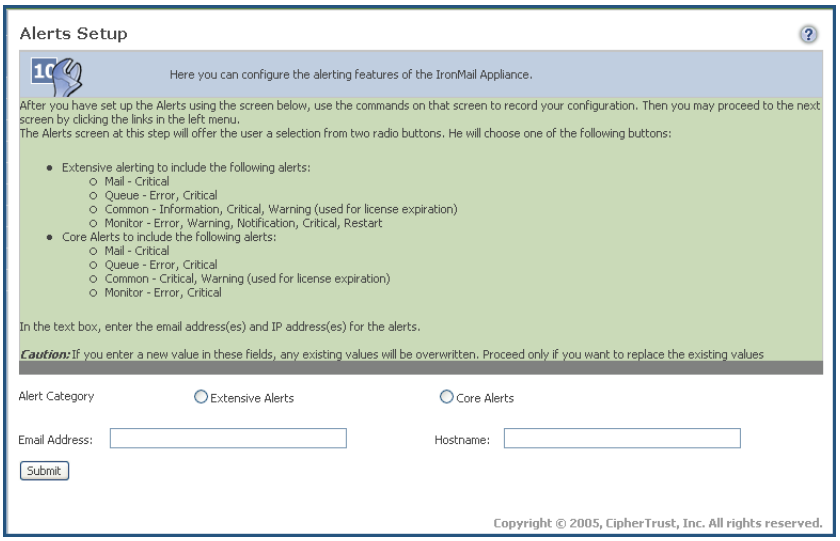

Report Setup
Here you can configure the reporting features of the IronMail Appliance.
After you have set up the Reports using the screen below, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking the links in the left menu. The Reports screen that will show at this step will offer the user a selection from two radio buttons. He will choose one of the following buttons:
All reports - the recipient will receive both detailed and summary reports
Core reports - the recipient will receive Incoming report, Outgoing report, Executive Summary, Executive Report, Overall Spam Summary, Overall Virus Summary, Overall Compliance Summary
In the text box, the user enters the email address(es) for the reports, and the SMTP relay to which they are sent.
Caution: If you enter a new value in these fields, any existing values will be overwritten. Proceed only if you want to replace the existing values
Report Category
All Reports
Core Reports
Email Address:
Hostname:
Submit
Copyright © 2005, CipherTrust, Inc. All rights reserved.

SmartStart Report Setup

After you have set up the reports using the screen at the bottom of the SmartStart page, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking that screen's link in the left menu.

Screen 6: Alerts Setup

This screen allows you to configure the alerting features of your IronMail appliance.

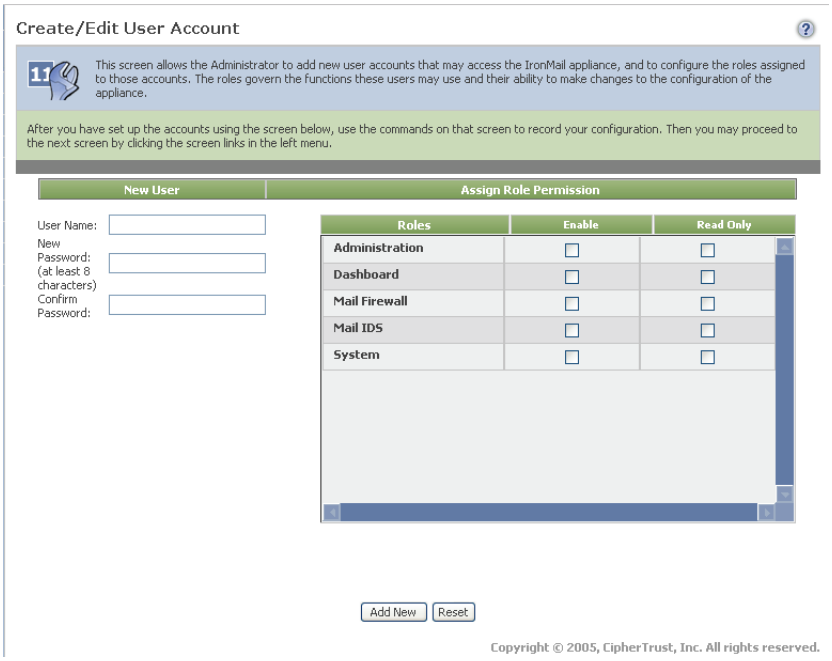

Alerts Setup
Here you can configure the alerting features of the IronMail Appliance.
After you have set up the Alerts using the screen below, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking the links in the left menu.
The Alerts screen at this step will offer the user a selection from two radio buttons. He will choose one of the following buttons:
Extensive alerting to include the following alerts:
Mail - Critical
Queue - Error, Critical
Common - Information, Critical, Warning (used for license expiration)
Monitor - Error, Warning, Notification, Critical, Restart
Core Alerts to include the following alerts:
Mail - Critical
Queue - Error, Critical
Common - Critical, Warning (used for license expiration)
Monitor - Error, Critical
In the text box, enter the email address(es) and IP address(es) for the alerts.
Caution: If you enter a new value in these fields, any existing values will be overwritten. Proceed only if you want to replace the existing values
Alert Category
Extensive Alerts
Core Alerts
Email Address:
Hostname:
Submit
Copyright © 2005, CipherTrust, Inc. All rights reserved.

SmartStart Alerts Setup

After you have set up the alerts using the screen at the bottom of the SmartStart page, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking that screen's link in the left menu.

Screen 7: Add Accounts

This screen allows the Administrator to add new user accounts that may access the IronMail appliance, and to configure the roles (permissions) assigned to those accounts.


Create/Edit User Account
This screen allows the Administrator to add new user accounts that may access the IronMail appliance, and to configure the roles assigned to those accounts. The roles govern the functions these users may use and their ability to make changes to the configuration of the appliance.
After you have set up the accounts using the screen below, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking the screen links in the left menu.
New User
Assign Role Permission
User Name:
New Password: (at least 8 characters)
Confirm Password:
Roles
Enable
Read Only
Administration
Dashboard
Mail Firewall
Mail IDS
System
Add New
Reset
Copyright © 2005, CipherTrust, Inc. All rights reserved.

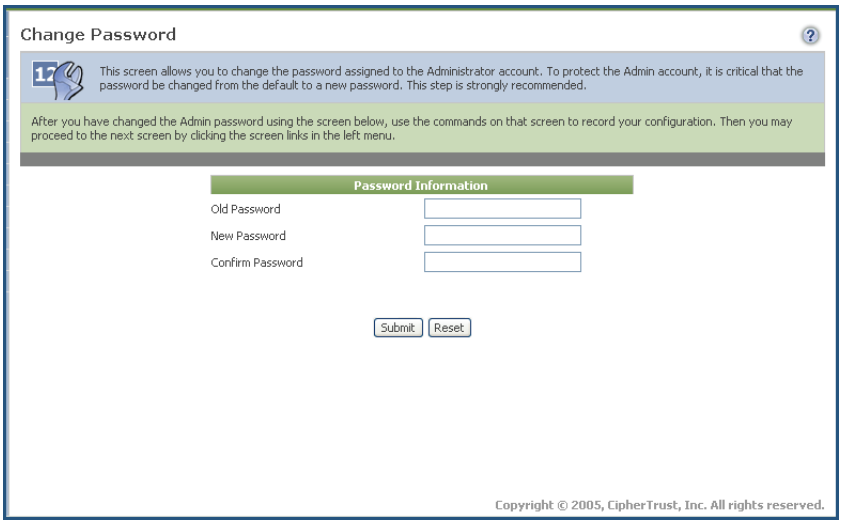
SmartStart Add Accounts

The roles govern the functions these users may use and their ability to make changes to the configuration of the IronMail appliance.

After you have set up the accounts using the screen at the bottom of the SmartStart page, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking that screen's link in the left menu.

Screen 8: Change the Admin Password

This screen allows you to change the password assigned to the Administrator account.


Change Password
This screen allows you to change the password assigned to the Administrator account. To protect the Admin account, it is critical that the password be changed from the default to a new password. This step is strongly recommended.
After you have changed the Admin password using the screen below, use the commands on that screen to record your configuration. Then you may proceed to the next screen by clicking the screen links in the left menu.
Password Information
Old Password
New Password
Confirm Password
Submit
Reset
Copyright © 2005, CipherTrust, Inc. All rights reserved.

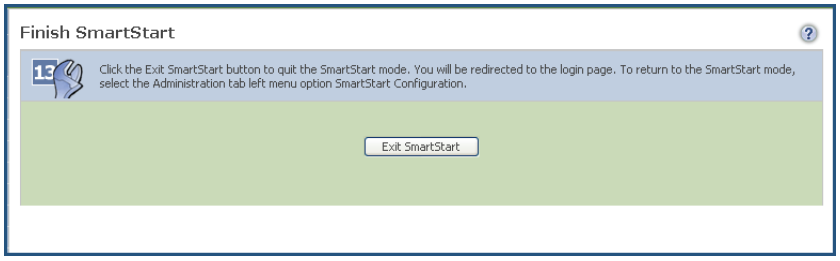
SmartStart Change Admin Password

IMPORTANT: To protect the Admin account, it is essential that the password be changed from the default to a new password. This step is strongly recommended.

After you have changed the Admin password on the screen at the bottom of the SmartStart page, use the commands on that screen to record your configuration. Then you may proceed to another screen by clicking that screen's link in the left menu.

Screen 9: Finishing SmartStart

This screen provides information that allows you to exit SmartStart gracefully, taking you back to the login screen.

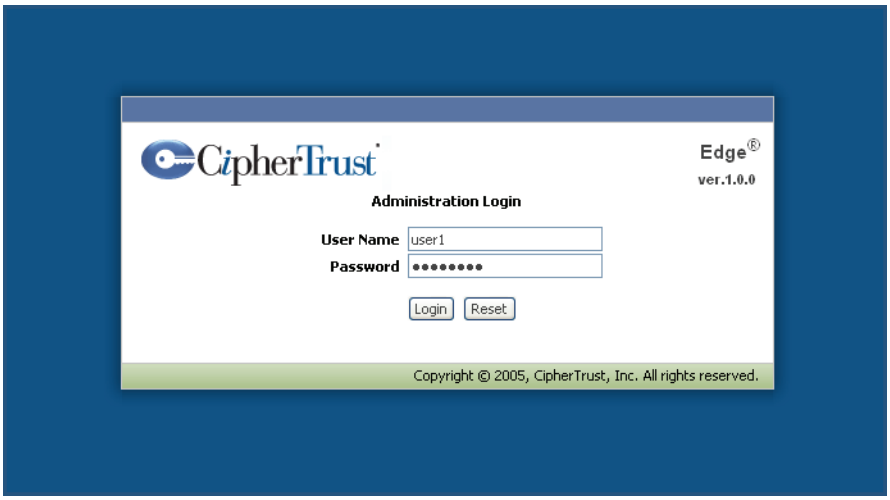

Finish SmartStart
Click the Exit SmartStart button to quit the SmartStart mode. You will be redirected to the login page. To return to the SmartStart mode, select the Administration tab left menu option SmartStart Configuration.
Exit SmartStart

Finish SmartStart

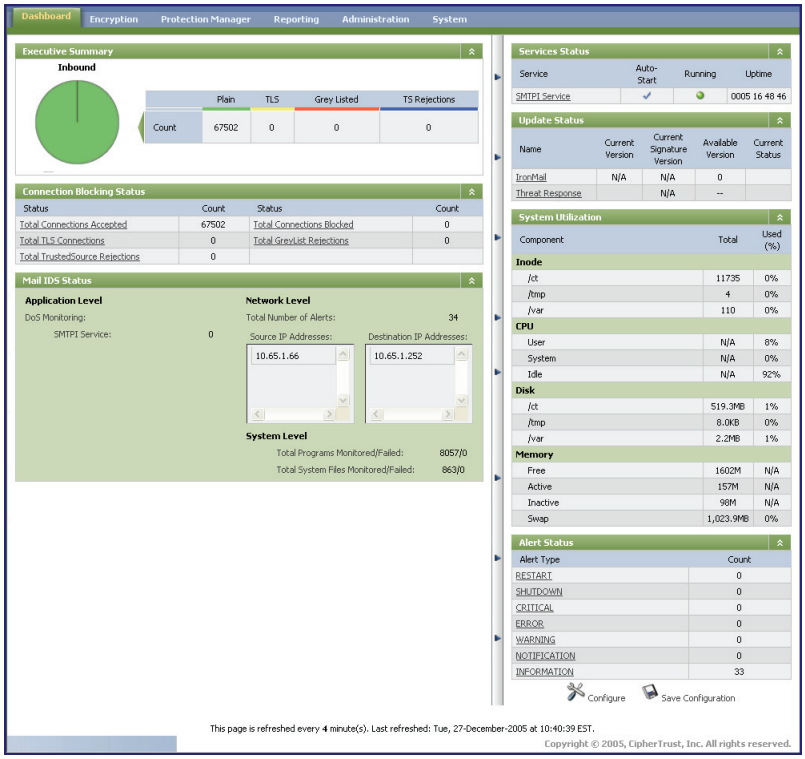
If you have finished SmartStart, click **Exit SmartStart** to proceed to the login screen.

When You Have Finished SmartStart

If you have applied all the steps of SmartStart, your IronMail appliance is now configured for deployment, using best practices configuration.



Log into IronMail using your user name and password, and you will see the IronMail Dashboard (IronMail's opening screen).



II: Monitoring the System

Any Administrator will tell you that one very important feature to any network protection solution is the provision of ways to monitor it. IronMail meets this requirement with the Dashboard, a one-page summary that allows the Administrator to easily review not only the status of the appliance and its components, but also its performance against all manner of attacks against the email network.

Using the Dashboard

IronMail's opening screen is the Dashboard, a customizable presentation of summaries and graphs that are intended to inform the user about IronMail's operation and performance. This section will explain how to set up the Dashboard as you want it to be, and inform you about each of the available summaries and graphs.

In this section: In this section you will find the following chapter:

- Chapter 3: The Dashboard.

The Dashboard

When a user logs onto IronMail, after the appliance has been deployed, the opening screen is the Dashboard. This configurable collection of tables and graphs allows the user to efficiently review the status and the performance of the system. The goal is to facilitate any decision-making that may be required, as well as to provide quick recognition of trends or of problems.

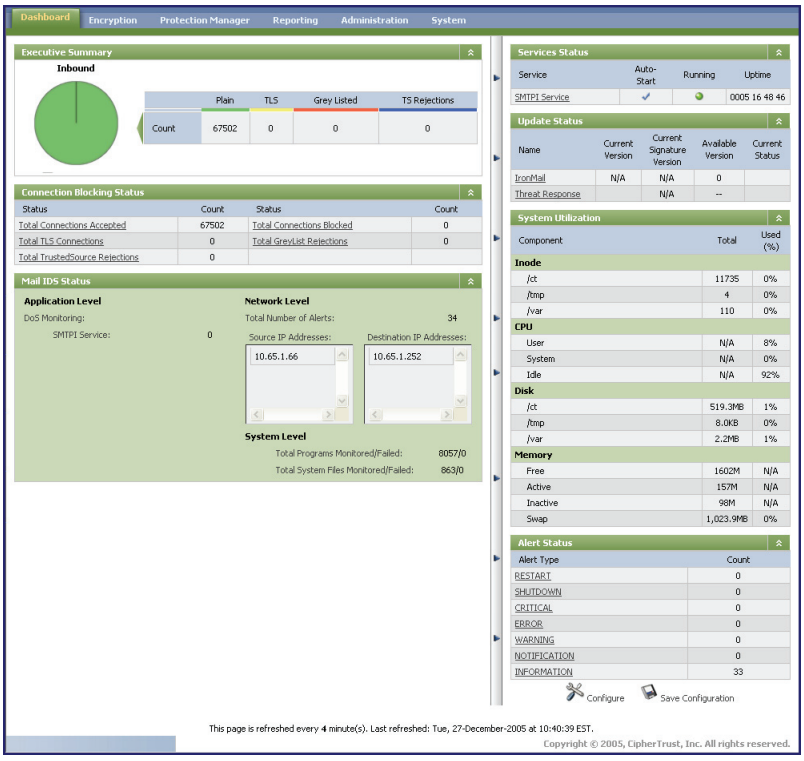
In this chapter

In this chapter you will find information about the following topics:

- The Dashboard Screen
  - Configuring the Dashboard
  - Configuring the Graphs

The Dashboard Screen

Logon > Dashboard

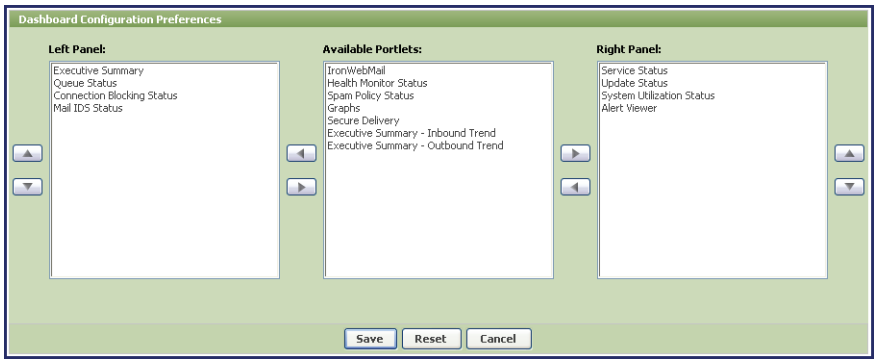


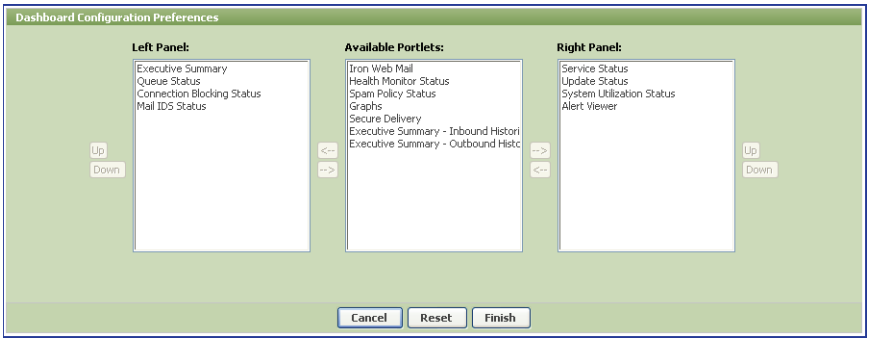
The Dashboard is the first screen the user sees when logging into IronMail.

Configuring the Dashboard

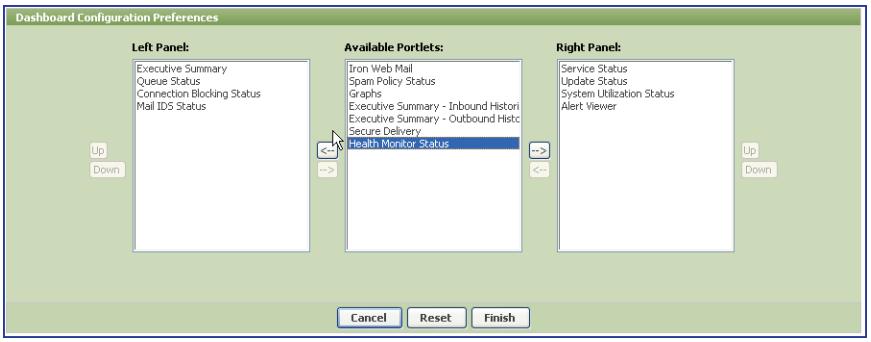
You can determine what summaries or graphs appear on your Dashboard, and where they are located, using the configuration screen. Click Configure at the lower right corner of the Dashboard screen.

Logon > Dashboard > Configure

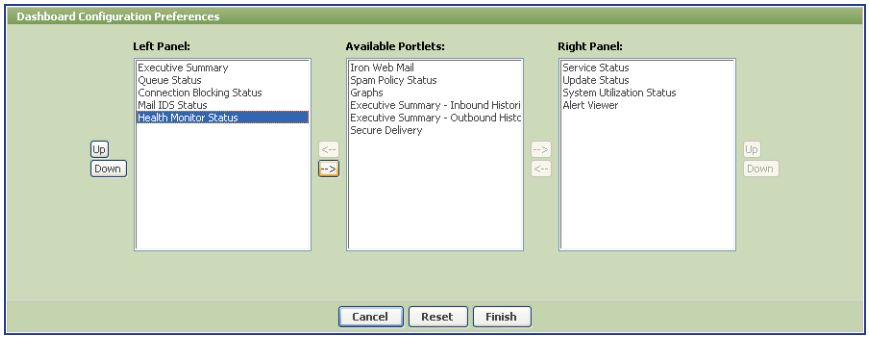




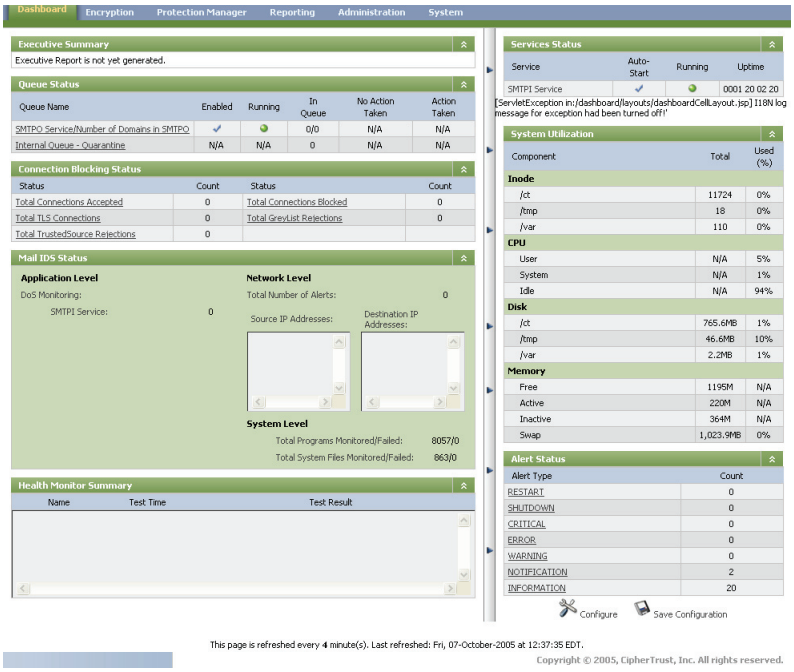
The center column of the Configure screen lists all portlets (each one representing a reporting mechanism) that have not been configured to appear on the existing Dashboard. To add a portlet to the Dashboard,, click the portlet to highlight it.



Then click the arrow pointing to the panel (**Left Panel** or **Right Panel**) where you want the new information to appear. The portlet will be moved to that panel, as shown below.



The new portlet is set to appear at the bottom of the panel, by default. If you want to change the placement of any portlet, highlight it and use the **Up** or **Down** button beside the panel. Click **Finish** to record the change.

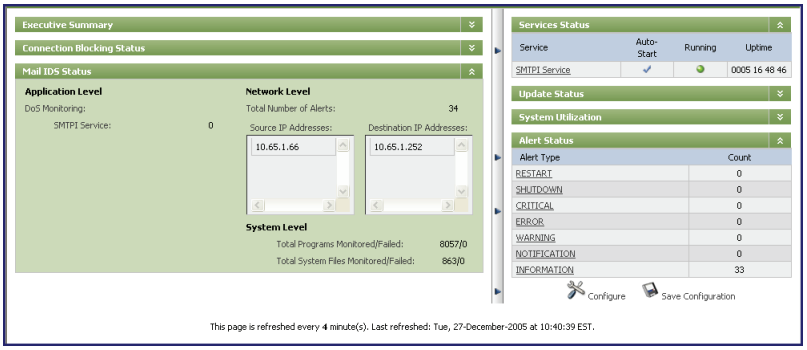


The Dashboard is now updated to include the Health Monitor Summary.

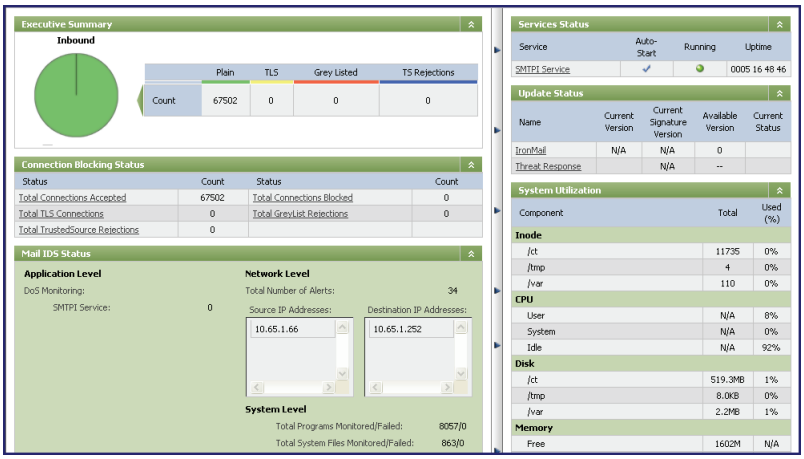
If you want to remove a portlet from the Dashboard, go to the Configure screen, highlight the portlet, and click the arrow pointing to the **Available Portlets** panel. When you click **Finish**, the portlet will be removed from its display panel and added to the **Available Portlets** list.

Special Navigation

You can expand or collapse any of the summaries that appear on the Dashboard, to allow focussing upon just the data you want to see. At the top right of each header, you will see double arrows, pointing either upward (when the summary is expanded) or downward (when the summary is collapsed.



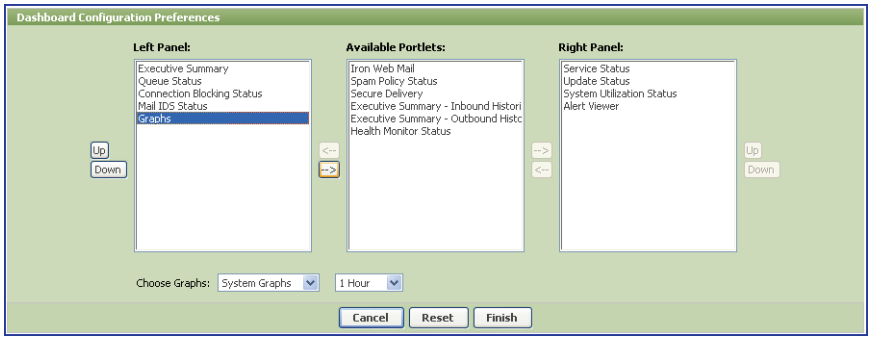
Clicking the double arrow icon toggles the summary between its collapsed and expanded states.



During the same login session, the Dashboard summaries will remain expanded or collapsed as you last left them. If you log out without saving the current configuration, the Dashboard will return to the configuration you found at login. If you do save the configuration before you log out, the Dashboard will remain as you last saw it before logout.

Configuring the Graphs

One of the portlets that appear on the Configure screen is labeled **Graphs**. This selection allows you to move a series of graphs onto the Dashboard, and to determine which of three possible sets of graphs you want to display.



Place the **Graphs** portlet in one of the display panels, just as you would any other portlet. When you click the arrow to move the portlet, the lower portion of the Configure screen displays two dropdown lists. The first list allows you to select which of the three types of graphs you want to display by default:

- System Graphs,
- Queue Graphs, or
- Executive Graphs.

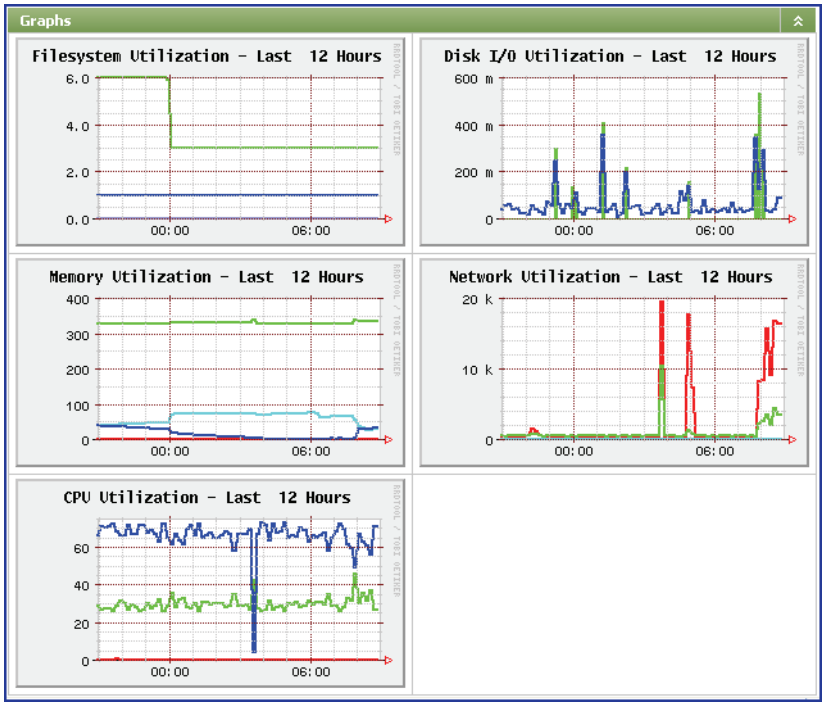
The second list offers selections for the time period you want to represent with the selected graphs. The available periods vary with the type of graph you select, so choose the type first.

More information about the information contained in each graph will be provided later in this chapter.

System Graphs

The System Graphs may be configured to capture system performance information for periods from 1 hour to 1 year.

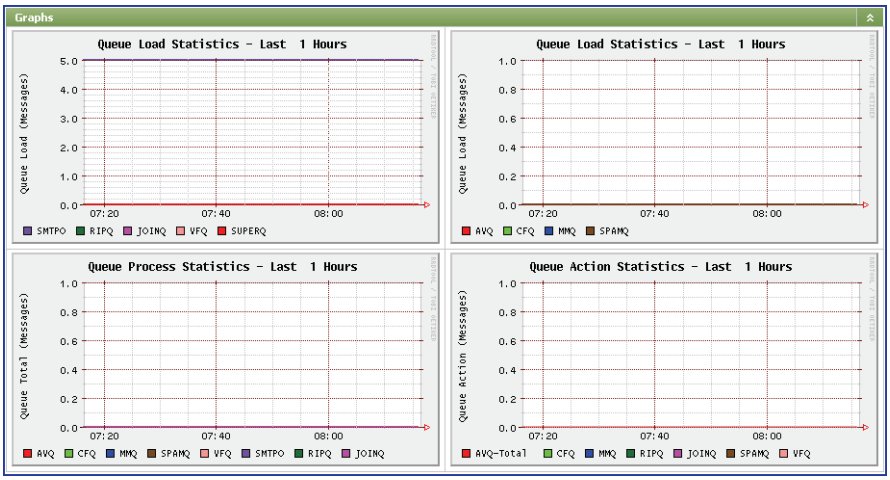
Logon > Configure > Graphs > System Graphs


Graphs
Filesystem Utilization - Last 12 Hours
Disk I/O Utilization - Last 12 Hours
Memory Utilization - Last 12 Hours
Network Utilization - Last 12 Hours
CPU Utilization - Last 12 Hours
00:00
06:00

Queue Graphs

The Queue Graphs may be configured to capture queue loads and performance information for periods from 1 hour to 1 year.

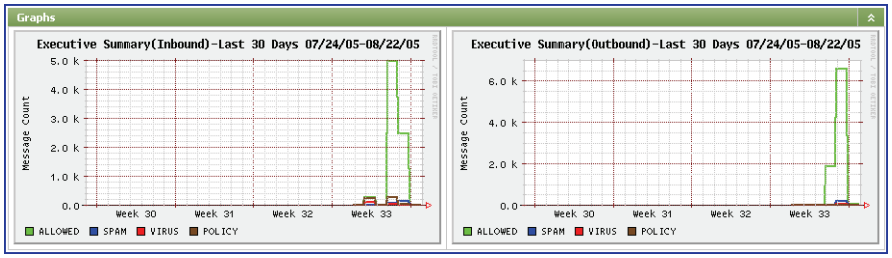
Logon > Configure > Graphs > Queue Graphs


Graphs
Queue Load Statistics - Last 1 Hours
Queue Load Statistics - Last 1 Hours
Queue Process Statistics - Last 1 Hours
Queue Action Statistics - Last 1 Hours
Queue Load (Messages)
Queue Total (Messages)
Queue Action (Messages)
07:20
07:40
08:00
SMTPO RIPQ JOINQ VFQ SUPERQ
AVQ CFQ MMQ SPAMQ
AVQ CFQ MMQ SPAMQ VFQ SMTPO RIPQ JOINQ
AVQ-Total CFQ MMQ RIPQ JOINQ SPAMQ VFQ

Executive Graphs

The Executive Graphs are intended to provide quick and accurate overviews of current system performance and activity, to allow the executive to spot trends and facilitate actions. The time periods available on the Executive Graphs are 1 week, 1 month, 3 months or 1 year.

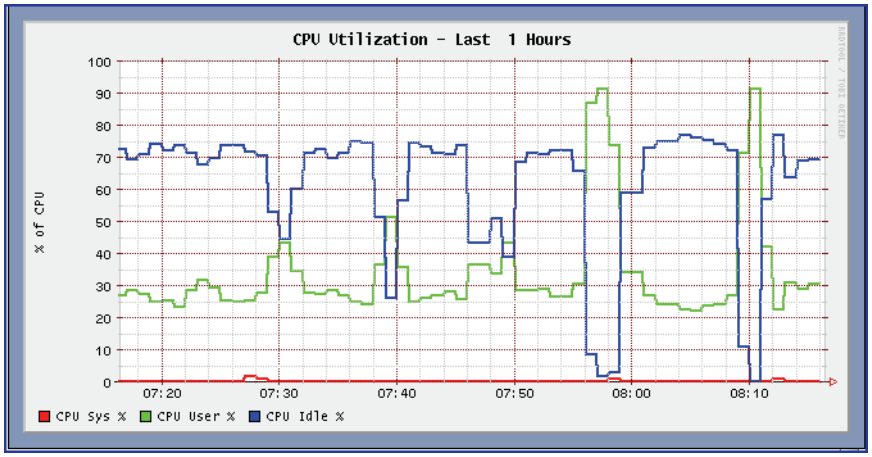
Logon > Configure > Graphs > Executive Graphs



When you have completed all settings, click **Finish** to record your changes. The Dashboard screen now displays the graphs you have selected, as well as the other portlets.

Special Navigation

If you wish to isolate any graph from the Dashboard, simply click on the graph you want to see. An enlarged copy of that graph will pop up, allowing you a better view of the data represented.



Saving the Configuration

IMPORTANT: When you have configured the layout of the Dashboard as you want it to appear, you must save that configuration. At the lower right of the screen, click the **Save Configuration** icon.

III: Encryption

Introduction

Current protocols governing email dictate that all messages transmitted over the internet be sent in plain ASCII text characters. The problem caused by this requirement is that anyone with the right tools can read a message sent by anyone else. The tools, such as TCP or packet sniffers, may be freely downloaded from the internet. The tools not only allow hackers to read anyone's email, but also allow them to intercept and alter the messages before they are delivered to the recipient. The easiest and most popular way for enterprises to secure their email is by using Digital Certificates.

These certificates allow two essential strategies for message encryption: "client to client" and "server to server" encryption.

In client-to-client encryption, Security Certificates are installed on individual workstations. The dominant benefit of this method is that the message is encrypted before it leaves the originator's computer and remains encrypted until it is received (protection from end to end).

Server-to-server encryption, on the other hand, requires Security Certificates be installed on the mail servers. Messages are protected only from server to server, not from the client to the server.

The following comparison illustrates the differences.

Comparing Strategies

Problem Area	Client-to-Client	Server-to-Server
Expense	Certificates must be purchased for and installed on every individual computer that will send and receive encrypted mail.	Only one certificate must be installed on the server; one server can encrypt and protect all email for client PCs in the domain.

Comparing Strategies

Problem Area	Client-to-Client	Server-to-Server
Administrative Workload	All certificates must be updated regularly, and may need to be uninstalled or transferred from one computer to another.	Administrators must manage only one certificate per gateway.
User Workload	Each user must tell all mail clients to user the certificates.	Encryption is transparent to the end user, and users cannot disable the encryption.
Scanability	Messages are encrypted before they reach the gateway. Therefore, they cannot be scanned for viruses, malicious content or confidential information, nor can the be scanned at the receiving gateway.	Messages may be scanned for viruses, spam, and email policy enforcement.
Encryption Security	Message body is encrypted, but header and routing information is not. Hackers have the opportunity to gain helpful information, and may be attracted by the encryption of the message body.	Establishes a secure tunnel between the sending and receiving email servers. Routing and encryption information is hidden.

IronMail's strategy provides the benefits of server-to-server encryption without permitting its drawbacks.

In this section

In this section, you will find the following chapter:

- Chapter 4: Managing Certificates

Managing Certificates

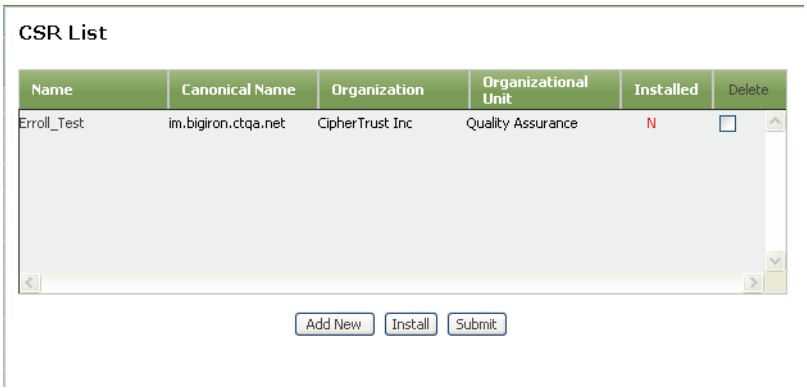
Certificates

IronMail provides an interface for requesting and installing a Security Certificate from a Certificate Authority. When a certificate is installed on the IronMail appliance, it is not necessary to install additional certificates on internal servers, unless the Administrator wants to protect the connection between IronMail and the internal servers and provide security for internal users sending or retrieving messages directly to or from the server. IronMail requires the installation of a Security Certificate so that administrative sessions with it via the Web Administration browser interface can be conducted securely.

X509 Certificates

IronMail requires the use of Security Certificates to provide secure services, much like banks or e-commerce web sites use them to provide secure connections for their web customers. The Certificate Signing Request (CSR) is actually the request made by an Administrator for a new certificate. Open the CSR List to see existing CSRs and to request new ones.

Encryption > Advanced > Certificate Management > X509 Certs > CSR List



The CSR List

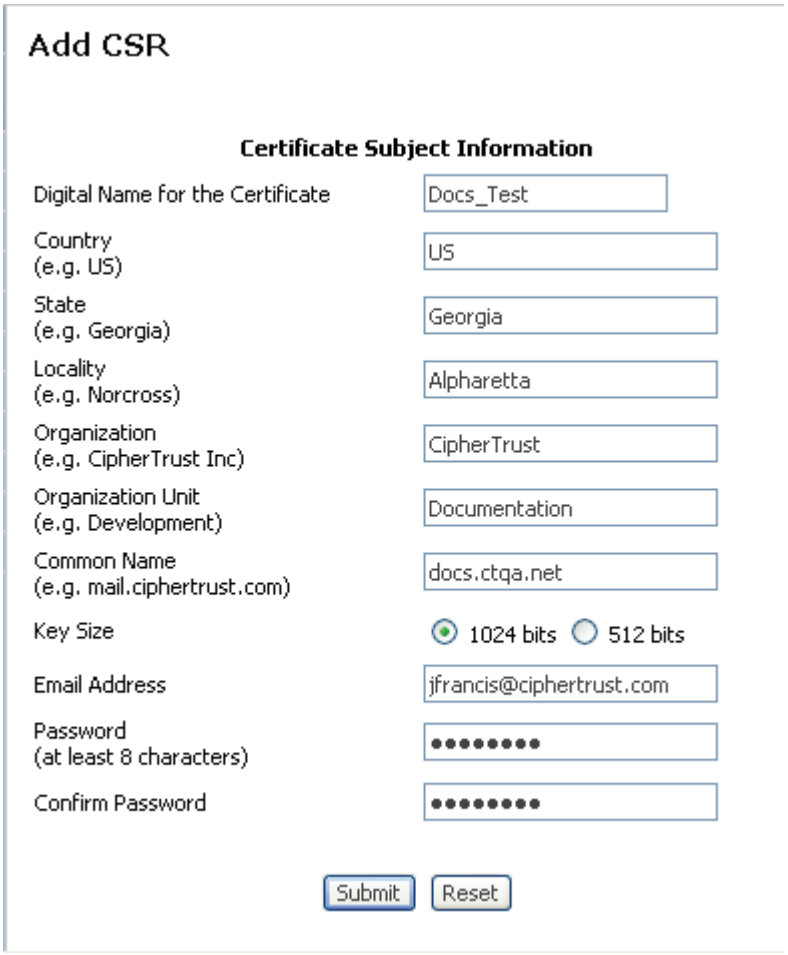
Field	Description
Name	This column shows the digital name for each CSR that has been processed and is awaiting installation.

The CSR List

Field	Description
Canonical Name	This column displays the canonical name for the server where the certificate will be installed. Example: mail.marketing.myplace.com
Organization	The name of the organization (e.g., CipherTrust, Inc.) that requested the CSR shows in this column.
Organizational Unit	This column lists the department or unit within the organization to which the certificate will be assigned (e.g., Development).
Installed	This column contains an N (for "not installed") until the certificate is installed.
Delete	Clicking the delete checkbox associated with any CSR and clicking **Submit** will delete that CSR. Clicking the Delete hyperlink will delete all CSRs.

Adding a CSR

Clicking the Add New button at the bottom of the CSR List screen opens the Add CSR screen. This screen allows you to generate a Certificate Signing Request.



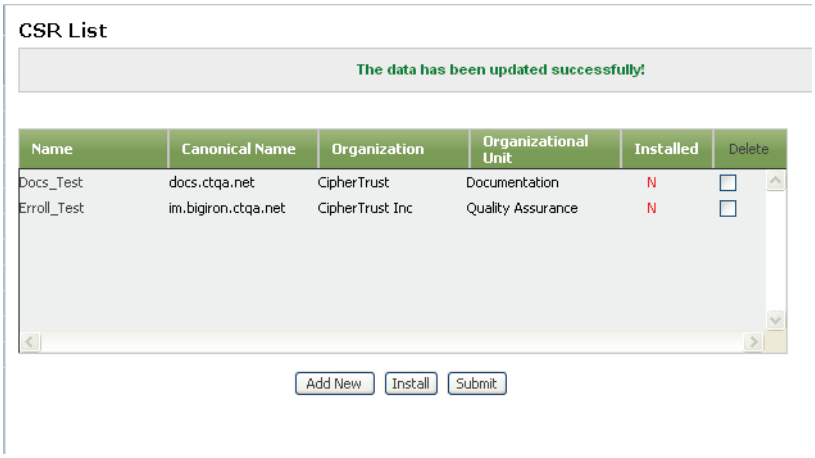
Adding a CSR

Field	Description
Digital Name for the Certificate	Enter the digital (displayed) name for the new certificate being requested. ***Note: :*** In order for the CSR to be generated, this name *cannot* contain spaces.
Country	Enter the name or abbreviation for the country where the certificate is to apply.
State	Enter the state name.
Locality	Enter the name of the locality.
Organization	Enter the name of the organization requesting the certificate.

Adding a CSR

Field	Description
Organization Unit	If applicable, enter the name of the unit within the organization to which the certificate will be assigned.
Common Name	Enter the server name where the certificate will be installed.
Key Size	Select the appropriate key size, in bits, for the public key to be installed. Options are: • 1024 bits • 512 bits The larger key is more secure, but is slower to process.
Email Address	Enter the email address for the Administrator for the certificate.
Password	Enter the password to be used by the Administrator to maintain the certificate.
Confirm Password	Confirm the password by entering it again.

When you have completed the necessary information, click Submit. The CSR List will refresh to add your new CSR.



IronMail will generate a private key/public key pair, and display in a text string the public key to be submitted to a "trusted root" source (such as VeriSign) for Security Certificates. Open a second browser window to navigate to a Security Certificate-issuing source.

Copy and paste the IronMail-generated text string into the appropriate input field of the Certificate Authority's web page when applying for a Certificate. When copying and pasting the key information, include the

"- - - - -BEGIN CERTIFICATE REQUEST- - - - -" AND "- - - - -END CERTIFICATE REQUEST- - - - -"

at the beginning and end of the IronMail-generated text string.

Note: When you go to the Verisign web page to get your certificates, you will be asked what platform you plan to use. Select **Apache**. If you choose Windows or IIS, the certificates you download will not work with IronMail appliances.

When you click Submit, the CSR is submitted to the Certificate Authority (CA). IronMail creates and stores a private key/public key text string in its database. When this string is submitted to a CA after the administrator completes and submits the CSR a second time, the issuing authority generates a new public key string. The new certificate information appears in the CSR List.

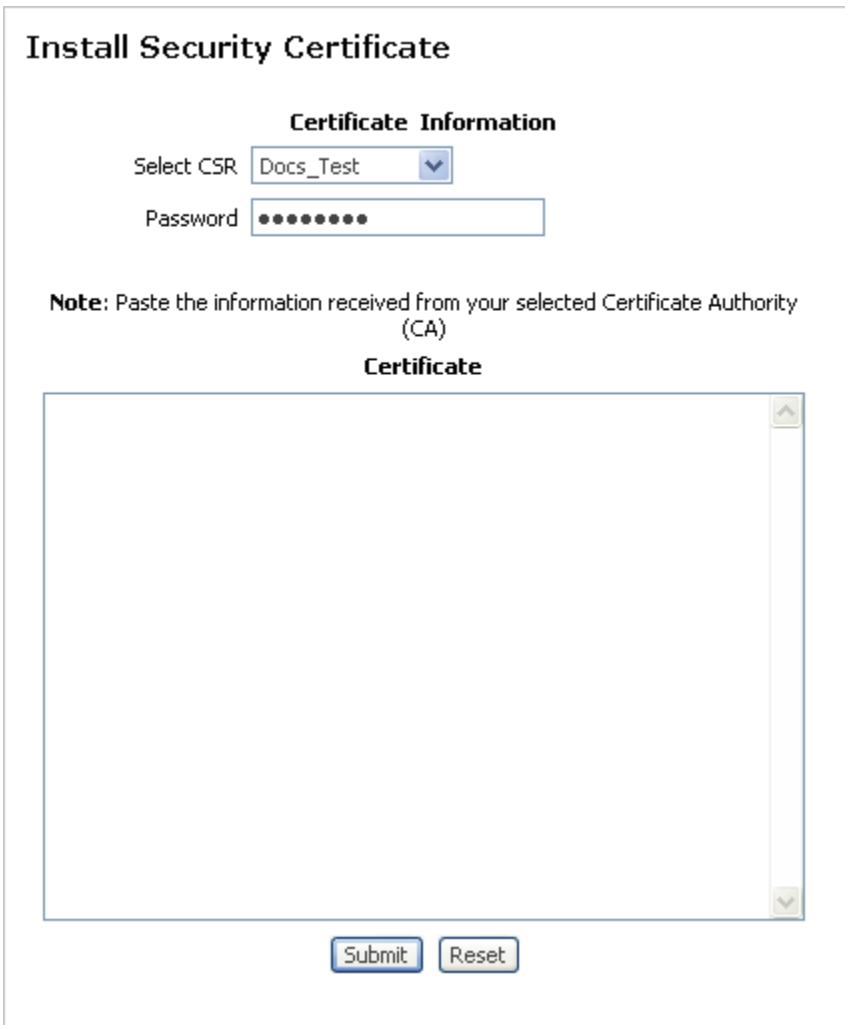
The install procedure allows you to paste this string in the IronMail Certificate section of the Install Security Certificate window and complete the certificate generation.

Installing an X509 Certificate

IronMail is pre-configured with an unsigned certificate in order to immediately provide secure SSL connections required for administrative sessions with the Web Administration interface. While the invalid certificate does allow encryption of email messages, that security is minimal because IronMail will not be able to authenticate itself to other servers, which may refuse to send messages to it. Therefore, in order to provide genuine security, a valid Security Certificate must be installed.

When the Certificate Authority returns the necessary certificate information, click **Install** on the CSR List screen. The Install Security Certificate window opens.

Encryption > Advanced > Certificate Management > X509 Certs > CSR List > Install



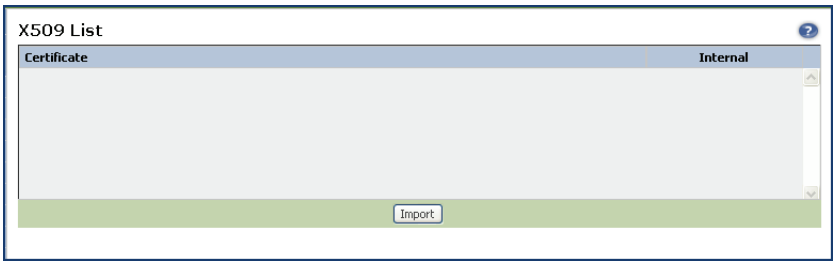
From the picklist, populated from the CSR List, select the certificate that is to be installed. Enter the password that was used to request the CSR from the Certificate Authority (CA). Then copy and paste into the Certificate input field the Security Certificate text string provided by the CA. Click **Submit**. The certificate will be installed, and the CSR will disappear from the CSR List.

Note: Installed Security Certificates cannot be uninstalled.

Storing X509 Certificates

When a certificate is installed, it is added to the X509 List. Storing the available certificates allows them to be archived for backup purposes. X.509 Certificates are added from the CSR list when they are installed.

Encryption > Advanced > Certificate Management > X509 Certs >Certs Store



The X509 List

Field	Description
Certificate	The name of each installed certificate will appear in this column.
Internal	For each certificate on the list, an Export hyperlink appears in this column.

Exporting an X509 Certificate

Because the Security Certificate may cost a considerable sum of money, IronMail provides a mechanism allowing administrators to "archive" a copy of it for safekeeping. Additionally, the public key of installed SSL and S/MIME Security Certificates may be exported to disk so they may be shared with trusted domains.

To export from certificate storage in the X509 List, click the Export link for the certificate you want to store. The Export Security Certificate screen displays.

Exporting an X509 Certificate

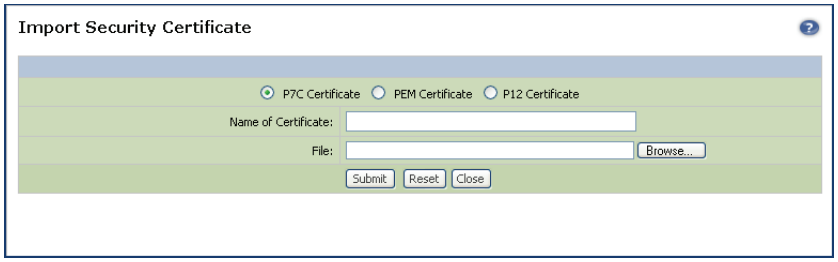
Field	Description
Certificate	Enter the name of the certificate to be exported.
Certificate Type	From the pick list, select the certificate type. Options are: • P7 - This contains the *public key* of a selected X509 Security Certificate in "P7C" format. This file may be shared with other domains to provide for message encryption. The domain's server will specify which format is required. • PEM - This contains the *public key* of a selected SSL or S/MIME Security Certificate in "CER" format. This file may be shared with other domains to provide for message encryption. • P12 - This file contains both the private key and public key of the Certificate in a format required for installing on another IronMail appliance. *Never distribute this file to another domain!*
Password	Enter the password used to request the certificate. This password will also be used to import the certificate if that becomes necessary.

Importing an X509 Certificate

To import an X.509 certificate, click the Import button at the bottom of the X509 List screen. The Import Security Certificate screen displays. The specific screen to use will depend upon what type of X509 certificate you want to import. The P7C, PEM and P12 screens appear below.

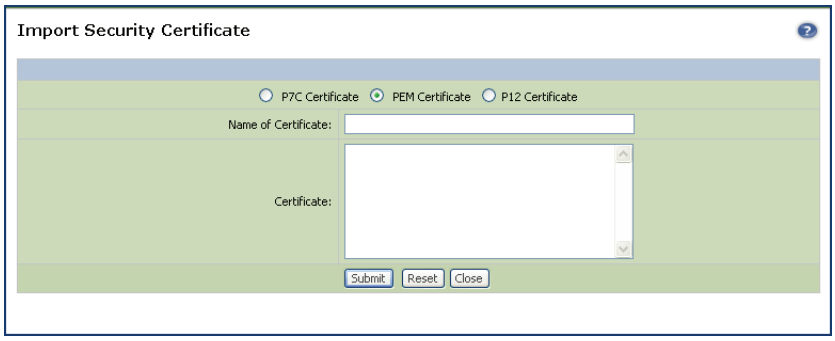
Note: P7C and PEM Certificates involve public keys only. No password is required. Simply enter the information required, browse to the file location where the certificate is stored (for P7C) and click **Submit**.

Encryption > Advanced > Certificate Management > X509 Certs > Certs Store > Import



Importing a P7C Certificate

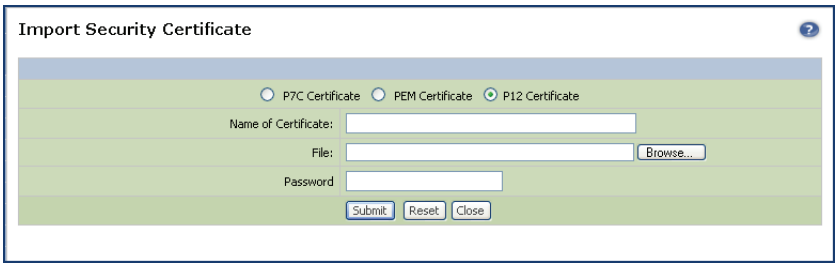
Field	Description
Certificate Type	Select the correct radio button to identify the certificate type (in this case, P7C). The screen will refresh to provide the correct data fields.
Name of Certificate	Enter the display name of the certificate.
File	Enter the path to the stored certificate or browse to it.



Importing a PEM Certificate

Field	Description
Certificate Type	Select the correct radio button to identify the certificate type (in this case, PEM). The screen will refresh to provide the correct data fields.
Name of Certificate	Enter the display name of the certificate.
Certificate	Paste in the certificate information as it came from the Certificate Authority.

For the P12 Certificates, a password is required, since the certificate contains both public and private keys. Enter the certificate name, browse to the file storage location, and enter the password that was associated with the certificate at the time it was exported. Click **Submit**. The imported certificate will appear on the X.509 List.



Importing a P12 Certificate

Field	Description
Certificate Type	Select the correct radio button to identify the certificate type (in this case, P12). The screen will refresh to provide the correct data fields.
Name of Certificate	Enter the display name of the certificate.
File	Enter the path to the stored certificate or browse to it.
Password	Enter the password associated with the certificate.

IV: Protection Manager

The network perimeter is, for most corporations, relatively secure. Firewalls, combined with a handful of other tools such as intrusion detection systems (IDS), have established a solid line of defense for corporate networks. In fact, firewalls have been so successful that most attackers have ceased trying to attack them. Instead, hackers are shifting their attacks to areas unprotected by traditional network security tools—to applications such as mail server and web server software. Hackers have learned to use actual email and email protocols as the "carriers" of, or vehicles for, their attacks. Email systems are being widely exploited in order to disrupt and violate corporate networks.

CipherTrust has taken a comprehensive approach to protecting corporations from email risks by providing an integrated solution, deployed at the gateway, which secures every aspect of the email system. It created IronMail, the secure email gateway appliance.

Controlling the Gateway

The first step to achieving email security is control of the gateway. Control the gateway and you protect the entire email infrastructure sitting behind it. But the range of threats targeted at email systems makes control of the gateway difficult. A comprehensive gateway security system must be capable of scrutinizing every attempted Internet connection to your internal servers, as well as the email messages themselves, ensuring that nothing harmful gets through. Such security must be able to stop a hacker's malicious code, a self-propagating worm, or even a dirty joke. If the gateway is secure, attacks never reach the mail servers. IronMail provides this security by fortifying the gateway and scrutinizing everything that attempts to pass through it.

Gateway Threats

Three primary threats plague enterprises if they are allowed to enter through the network gateway:

- Denial of service attacks;
- Intrusions; and
- Web mail attacks.

IronMail provides state-of-the-art solutions for each.

Denial of Service

Hackers may launch denial-of-service attacks against e-mail systems in an attempt to bring those systems to a halt. Many techniques are capable of accomplishing this disruption, but hackers typically exploit vulnerabilities in a mail server, such as the inability to process a malformed MIME message or buffer overflow constraints. Or the attackers

can simply flood a mail server with more SMTP connections or instructions than the server can handle.

Intrusions

Intrusions occur when unauthorized users gain access to the organization's infrastructure. For spammers, this typically means breaking into a mail server to send spam (mail relay) or to harvest e-mail addresses. Spammers can also plant computer code on the organization's personal computers, which then become spam machines or drones. Recent worms and viruses are examples of the results from intrusions.

Web Mail Attacks

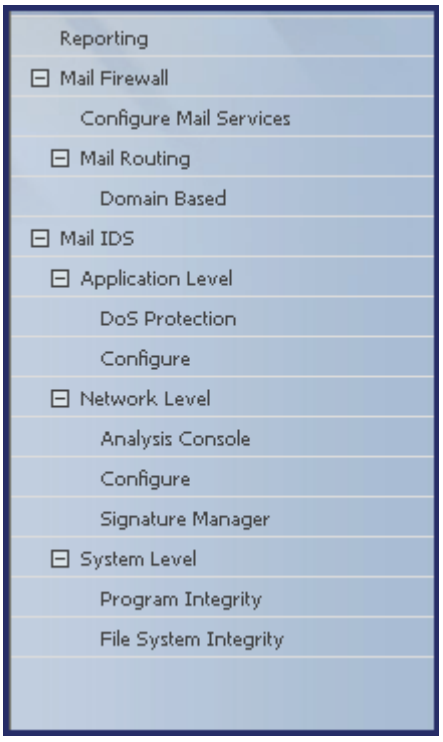
Many enterprises allow their mobile workers to access corporate e-mail through applications such as Outlook Web Access (OWA) or iNotes. Web mail requires a web server, which is subject to numerous vulnerabilities, blended threats, viruses and worms.

IronMail is a hardened e-mail gateway appliance that acts as an application-specific firewall. It allows only valid and safe connections to e-mail servers.

In this section

In this section you will find the following chapters:

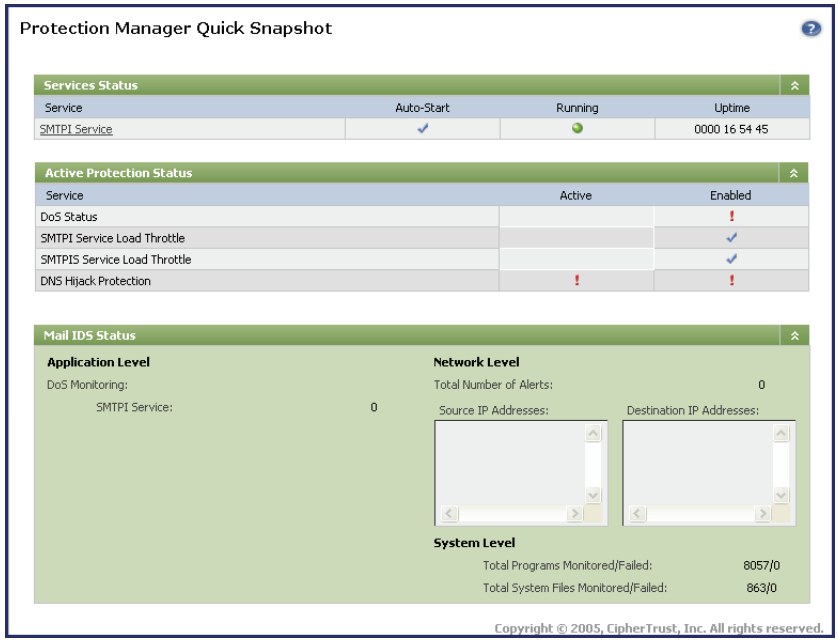
- Chapter 5: Mail Firewall
- Chapter 6: Mail-IDS



Available Reports

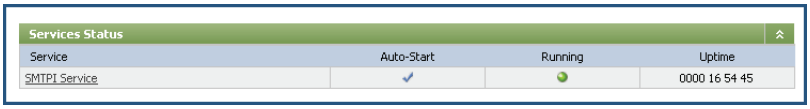
The first screen that appears when Protection Manager opens is the Protection Manager Quick Snapshot. This report screen consists of three panels containing tables that provide current information about processes within this program area.

Login > Protection Manager



Services Status

The top panel provides data about a variety of services, configured by specific functions within IronMail



Services Status

Field	Description
Service	This column lists the various mail services that are being monitored. Each service name is also a hyper-link that opens the specific service properties screens for the service in question.

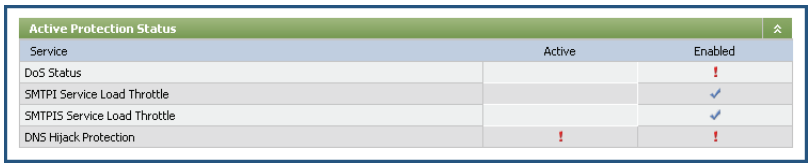
Services Status

Field	Description
Auto-Start	This column indicates for each service whether or not it is configured to be started automatically if it is not running when it is checked by Health Monitor. A check mark indicates the service is configured to restart. And X indicates it is not so configured. Clicking the current symbol will toggle the configuration to the other status.
Running	A green light icon in this field indicates the service is currently running. A red icon indicates it is not running. Clicking the icon will toggle the service off and on.
Uptime	This column displays the time in days, hours, minutes and seconds the service has been running since it was last started.

Active Protection Status

This table tracks the current status of four forms of active protection;

- Denial of Service protection
- SMTPI Service load throttling
- SMTPIS Service load throttling
- DNS Hijack protection



Active Protection Status

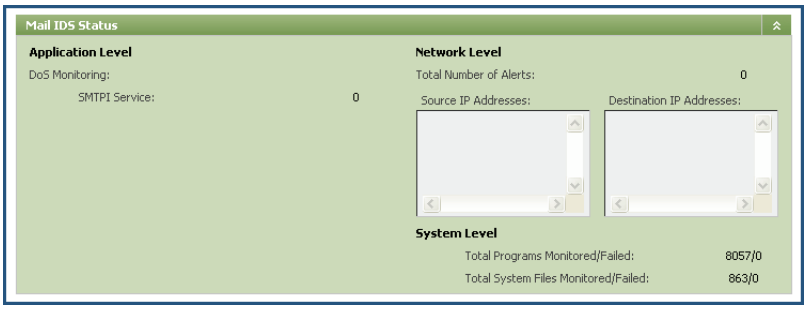
Field	Description
Service	This column lists the services by name.
Active	If the service is currently in operation, that fact is indicated by an icon in this column.
Enabled	Icons in this column indicate if the service is enabled or not. A check mark indicates the service is enabled; an exclamation point indicates it is not.

Mail IDS Status

The Mail IDS Status section tracks results of intrusion detection tools at three levels:

- Application Level

- Network Level
- System Level



Mail IDS Status

Field	Description
Application Level	*This area reports the results from Application Level Protection tools.*
DoS Monitoring	This field includes reports of Denial of Service attacks on three different services. A number of detected attacks since midnight will show for each service. The services are: • SMTPI • POP3 • IMAP4 The DoS Monitoring label is a hyperlink that opens the DoS Protection screen. Each service label is a hyperlink that will take you to the associated service properties screen.
Anomaly Detection Engine	This field will report any violations of anomaly detection rules. The name is also a hyperlink that opens the Show Anomaly Detection Rules screen.
Network Level	*This area reports the results from Network Level Protection tools. Any of the field labels is a hyperlink that will take you to the Analysis Console screen.*
Total Number of Alerts	This field displays the total number of alerts sent since midnight.
Source IP Addresses	The source IP addresses for the emails that generated alerts display in this list.
Destination IP Addresses	This list shows the destination IP addresses to which the offending emails were addressed.
System Level	*This area reports the results from System Level Protection tools.*

Mail IDS Status

Field	Description
Total Programs Monitored/Failed	This field contains the results of the last Program Integrity check, in terms of the number of programs checked and the number that failed the check.
Total System Files Monitored/ Failed	This field contains the results of the last File System Integrity check, in terms of number of files checked and the number that failed.

Mail Firewall

As a proxy, IronMail scrutinizes every attempted connection to your mail servers, detecting and blocking all known or potentially harmful connections. IronMail employs CipherTrust's patented Mail-Firewall® technology to deliver the most robust email gateway protection available.

In this chapter

In this chapter, you will find information about the following topics:

- Mail Services
  - Configure Mail Services
- Mail Routing
  - Domain-Based Routing

Mail Services

IronMail implements three services or "subsystems" to process messages transmitted via the SMTP email protocol.

- The **SMTPI Service** processes messages coming into the IronMail appliance via port 25. (The "**I**" signifies "coming **I**nto IronMail.") New IronMail users frequently confuse "incoming messages" with messages coming into the network from the Internet. In fact, the SMTPI Service processes all messages coming into the IronMail appliance, whether originating inside or outside the local network (see SMTPI/SMTPIS Services).
- The **SMTPO Service** processes all messages that IronMail delivers out of the appliance. (The "**O**" represents "delivered **O**ut of IronMail.") Again, new IronMail users mistakenly think of the SMTPO Service as the subsystem that delivers email originating within the network to users out in the Internet. While this is true, it is more correct to understand that the SMTPO Service delivers all messages out of the appliance, whether their destination is inside or outside the network (see SMTPO Service).

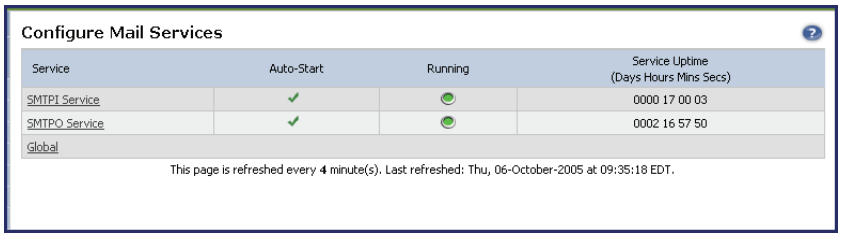
Invisible to the IronMail administrator is the SMTPI and SMTPIS Services' enforcement of the SMTP protocol. Before these services will accept the data or "payload" of an email, they inspect the requested email connection at the application level to ensure that it is legitimate. Connection requests that do not conform to the SMTP protocol are dropped. If the connection is accepted, then IronMail processes the message like a full-featured mail server application. Accordingly, the

SMTPI/S Services have many configuration options that affect how they process and deliver messages.

Configure Mail Services

The Configure Mail Services table contains four columns: **Service**, **Auto-Start**, **Running**, and **Service Uptime**.

Protection Management > Mail Firewall > Configure Mail Services



Configure Mail Services

Field	Description
Service	This column contains the names of the IronMail services or subsystems that process SMTP email delivery. (An entry in this column named “Global” allows configuration options that do not strictly fall under the SMTPI or SMTPO Services.) Each service name is a hyperlink that allows configuration of that service.
Auto-Start	A red X or green check icon indicates whether or not the service is set to start automatically when the IronMail appliance is rebooted. If an icon is green, the service will begin running when IronMail restarts. In addition, if the icon is green, IronMail’s Health Monitor will restart any service except SMTPO that has stopped for any reason when it performs its tests on all appliance subsystems. If an icon is red, the service will not start on reboot, nor when Health Monitor runs its system tests. (Note that a service can continue to run after its auto-start setting is turned off.) The red and green light icons are hyperlinks. Clicking the icon/hyperlink toggles the auto-start option on and off.
Running	A red or green light icon indicates whether or not the service is currently running. (Note that in some situations, the **Running** icon may not refresh when clicked, i.e. change from green to red. If the icon does not toggle as expected, click the Configure Mail Services hyperlink in the left navigation frame of the Web Administration interface to refresh the page, rather than clicking the **Running** icon a second time.)

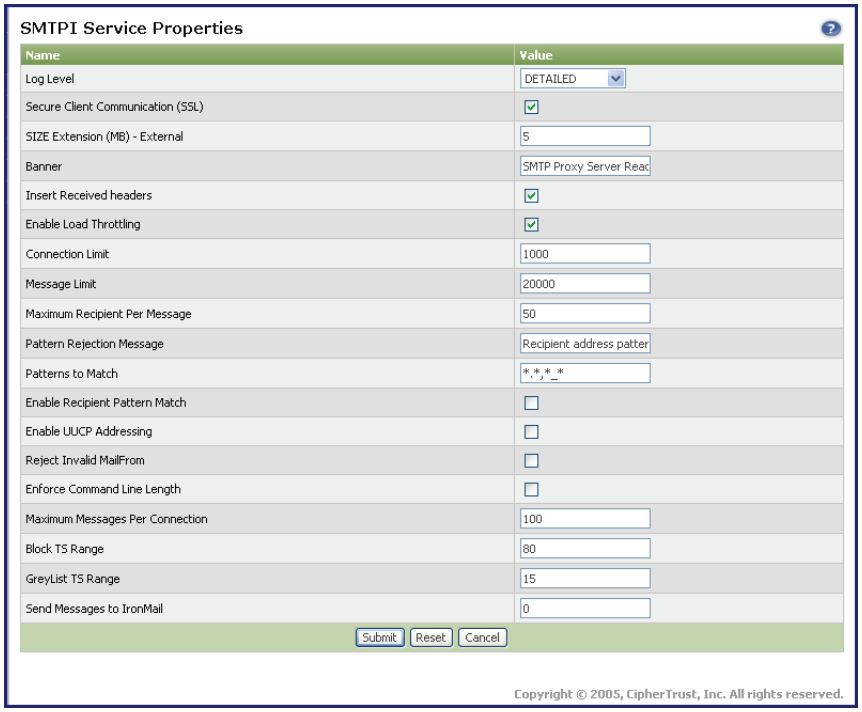
Configure Mail Services

Field	Description
Service Uptime	This column indicates (in days, hours, minutes, and seconds) how long a service has been running since it was last restarted. If the "uptime" appears less than expected, it may indicate that the service was manually stopped and restarted by an administrator, or was stopped by an administrator and was restarted automatically by IronMail's Health Monitor.

SMTPI Service

Clicking the SMTPI name hyperlink opens the SMTPI Service Properties screen.

Protection Management > Mail Firewall > Configure Mail Services > SMTPI



The following configuration options are available:

SMTPI Service Properties

Field	Description
Log Level	IronMail generates detailed logs that record the activities of all its subsystems. The detailed logs may be saved to disk and sent to CipherTrust engineers for troubleshooting purposes. The Log Level set here determines the type and amount of detail written to the log. Select the proper log level from the drop down list. The options are: • Critical • Error • Information • Detailed Note that in high email-volume environments (50,000+ messages per day), the SMTPI Service's log can easily grow to 100 MB or more per day. If IronMail is not configured to delete these logs after 3-7 days, there is a danger that IronMail's hard disk can quickly become full.
Secure Client Communication (SSL)	Select this checkbox to enable secure communication between IronMail and the client servers. Valid only for SMTPI, not for SMTPIS, which is already secure.
SIZE Extension (MB) - External	Enter a number (in megabytes) representing the maximum email size IronMail will accept from users outside the domain(s) it hosts. If the message exceeds this size, IronMail will not accept it. A zero in this input field represents “unlimited”—there is no size limit.
Banner	In order to hide information about your email infrastructure that might be exploited by hackers, IronMail allows you to provide an alternate Welcome Banner. The banner is limited to 80 characters, and may not contain “new line” characters.
Insert Received Headers	With this option enabled, IronMail will add to every email's header an RFC822-compliant reference to its own role in the delivery of the message.

SMTPI Service Properties

Field	Description
Enable Load Throttling	IronMail has a very powerful and efficient "engine" capable of processing tens of thousands of messages very quickly. However, in very high email environments, or during times of peak volume, IronMail can dynamically "throttle" the rate of incoming connections based on how many messages have already been received and are still in the process of being examined. As the number of unprocessed and "still-being-processed" messages grows, the SMTP Service will begin lowering the numbers of simultaneous email connection requests it accepts. When IronMail reaches an administrator-defined "maximum message load" (see immediately below), the SMTP Service drops to its default low-acceptance rate of three simultaneous connections (see the Load Throttling graphic below). As the message load decreases, the rate of simultaneous incoming SMTP connections increases again. When IronMail's load throttling is in effect, users trying to send mail to domains IronMail hosts will receive a "421: Server busy. Try again…" alert message in their email client if their connection is refused. The load throttling parameters are established by the **Connection Limit** and **Message Limit** fields that follow.
Connection Limit	Enter a number between 100 and 500 to represent the maximum number of simultaneous incoming connections allowed when Load Throttling is enabled.
Message Limit	Enter a number (500-50,000) representing IronMail's "maximum message load." (A zero is not allowed in this field.) When this number of "not yet processed" and "in-process but not yet delivered" messages is present in IronMail's Message Store, the SMTP Service will drop to its lowest connection acceptance rate of three simultaneous connections. Load throttling gracefully slows the number of accepted simultaneous connections, from the number established as the "Connection Limit" down to a default low of three simultaneous connections, depending on how closely the number of messages in the Message Store approaches the Message Limit specified here.

SMTPI Service Properties

Field	Description
Maximum Recipient per Message	Enter a number (25-500) representing the maximum number of recipients to which an email may be addressed. (The SMTPI Service totals the sum of all recipients, regardless of whether they are contained in the TO, COPY, or BLIND COPY fields.) For IronMail-to-IronMail communications, if an email is addressed to 200 addresses and the SMTPI recipient limit is set to 50, IronMail will accept the message and deliver it to the first 50 recipients submitted by the sending server. The SMTPI Service will not deliver the message to the 51st recipient and beyond. If the email is received from a non-IronMail server, the behavior can differ and IronMail may reject the entire message where the number of addresses exceeds the SMTPI limit.
Pattern Rejection Message	Enter the text that is to be part of the SMTP Failure (550) response (indicating that the Mailbox is unavailable) when an inbound recipient address does not match the specified patterns.
Patterns to Match	Enter the pattern or patterns that a recipient's email address is allowed to have. Either or both of the two patterns (*.* and *_*) are permitted. Patterns must be separated by a comma (,) with no space separation between the comma and the pattern.
Enable Recipient Pattern Match	This option enables pattern checking. Only two patterns are currently supported. The configured pattern(s) are used to inspect the unique message identifier (UID) part of the recipient email address: • * _* eg. *firstname_lastname*. The UID has at least one underscore "_" as in the recipient email address, james_smith@earthlink.com. • * .* eg. *firstname.lastname*. The UID has at least one period "." as in the recipient email address, account.manager@ciphertrust.com. By default this option is disabled. If this option is enabled, a pattern match check is performed using the patterns in the **Patterns to Match** field. If a pattern match occurs, IronMail returns an OK (250) reply response. Otherwise IronMail returns a Failure (550) reply.
Enable UUCP Addressing	If enabled, IronMail allows UUCP (Unix-to-Unix CoPy) addressing. UUCP is a computer program and protocol allowing remote execution of commands and transfer of files, email, and netnews between Unix computers. If disabled, IronMail rejects the recipient.

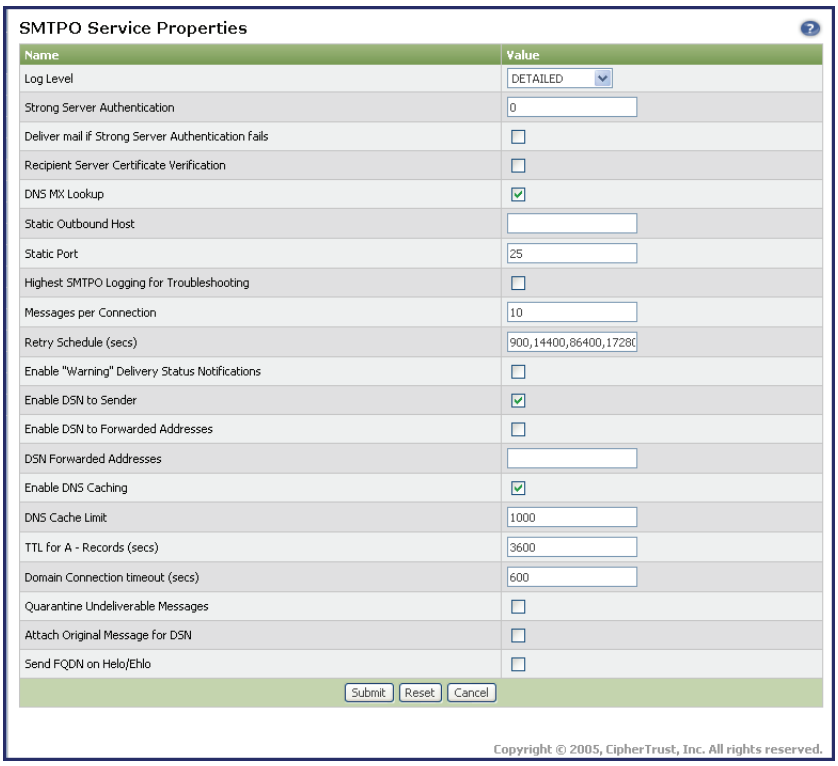
SMTPI Service Properties

Field	Description
Reject Invalid MailFrom	If enabled, as part of spoofed message protection, IronMail will reject mail from an address that is part of a routing domain, but is not in the Allow Relay IP addresses.
Enforce Command Line Length	IronMail will enforce RFC restrictions on the length of an SMTP command line to 512 characters, including carriage returns and line feeds.
Maximum Messages per Connection	Enter a number (0 - 50) to represent the maximum number of messages allowed per connection. Entering zero (0) enables an unlimited number of messages. The limit applies only to connections that do NOT have relay permission through IronMail.
Block TS Range	Enter a number between 15 and 150 to represent the TrustedSource threshold at which Edge will block an incoming connection.
Greylist TS Range	Enter a number between 1 and 80 to represent the TrustedSource threshold at which Edge will greylist an incoming connection.
Send Messages to IronMail	If enabled, this parameter will allow Edge to send the IP address of each message that passes through to the IronMail appliance. The IP addresses will be stored in the database so they may be viewed in the logs, etc. The only IP address the IronMail normally receives (if this parameter is turned off) is the IP for the Edge appliance. Enter a “1” to enable sending the addresses; enter a “0” to disable it. The default is “0.” ***Note:*** This feature may require modification on the IronMail appliance, in the form of a software patch, to allow the IP addresses to be stored, etc.

SMTPO Service

Whereas the SMTPI Service is responsible for processing messages entering the IronMail appliance (whether originating from inside or outside the hosted domain), the SMTPO Service is responsible for delivering the messages out of the appliance. Clicking the SMTPO Service hyperlink in the Configure Mail Services window opens a secondary screen where the following configuration options are available:

Protection Management > Mail Firewall > Configure Mail Services > SMTPO



SMTPO Service Properties

Field	Description
Log Level	IronMail generates detailed logs that record the activities of all its subsystems. The detailed logs may be saved to disk and sent to CipherTrust engineers for troubleshooting purposes. The Log Level set here determines the type and amount of detail written to the log. Select the proper log level from the drop down list. The options are: • Critical • Error • Information • Detailed Note that in high email-volume environments (50,000+ messages per day), the SMTPI Service's log can easily grow to 100 MB or more per day. If IronMail is not configured to delete these logs after 3-7 days, there is a danger that IronMail's hard disk can quickly become full.

SMTPO Service Properties

Field	Description
Strong Server Authentication	Receiving servers may have Security Certificates installed on them and support TLS. Yet the presence of a Security Certificate does not guarantee authenticity. Therefore, in accordance with the values entered in this input field, IronMail may refuse to deliver a message to any server that cannot “strongly” authenticate itself with a valid Security Certificate. There are three possible values for this option: • “ 0” (disabled, i.e. no authentication required) • “ 1” (require a Security Certificate, perform a TLS HandShake, and verify that the receiving server's host name the common name (host name) on the its security certificate.) • “ 2” (require a Security Certificate, perform a TLS HandShake, and verify that the receiving server's domain name matches the domain name on its security certificate.) **Note:** If a “1” or “2” is entered in this input field and the receiving server does not have a valid Security Certificate, the email will not be delivered unless the very next option, immediately below, is enabled. It is important to state very plainly: as long as there are few servers with installed Security Certificates, the chance that this option will cause valid email to be undeliverable will be very high. This option only becomes useful as increasing numbers of servers install valid Security Certificates. Therefore, IronMail administrators are cautioned to be judicious in their implementation of this option.
Deliver mail if Strong Server Authentication fails	If a value of “1” or “2” is entered in the “Strong Server Authentication” option above, and the host or domain name on the receiving server's Security Certificate cannot be authenticated, this option determines whether or NOT IronMail will deliver the message. If unchecked, messages will not be delivered when the Security Certificate cannot be authenticated. If checked, IronMail will deliver the message regardless of the certificate’s authenticity.

SMTPO Service Properties

Field	Description
Recipient Server Certificate Validation	If enabled, this option requires the strongest possible server authentication before sending messages: IronMail will validate the Security Certificate with the trusted "root" source that issued it. This verifies that the “root” of the receiving server's Security Certificate is a valid Certificate Signing Authority (CSA). If this option is enabled and verification fails, the connection will be dropped. If the option is disabled, a verification failure will be logged, but the connection is allowed and the message will be delivered. The “verification failure” event is logged in the “SMTPO Service” daily detailed log file.
DNS MX Lookup	If enabled, IronMail will use a DNS MX lookup to identify where to send email it is to deliver. IronMail uses the DNS servers whose IP addresses are listed in *System > Configuration > IronMail > “DNS-1,” “DNS-2,” and “DNS-3*.” If disabled, IronMail will deliver all email to the address in the **Static Host** field identified immediately below. (The **DNS MX Lookup** and **Static Host** options are only valid for messages that are delivered to external domains.) **Note** To prevent potential looping and blocking conditions, IronMail does not attempt delivery of email if the MX lookup returns the reserved IP address (0.0.0.0 or 127.0.0.1).

SMTPO Service Properties

Field	Description
Static Outbound Host	Instead of performing a DNS lookup and delivering messages accordingly, IronMail can send all messages to a specific host that may perform special processing or routing functions. (The host then becomes responsible for the delivery of messages.) Enter either the host name (e.g., "hostname.domainname.com") or IP address of the server where IronMail should deliver all its messages. (If entering a host name, IronMail must be able to resolve the name to the machine's IP address, i.e. DNS records must exist for it.) Note that domains and machine names in IronMail's routing table (*Mail-Firewall* > *Mail Routing* > *Domain-based*) take precedence over the route that is specified here in the SMTPO properties window. Any messages addressed to a domain listed in the Domain-based routing table will be delivered directly to that domain's mail server, rather than to the Static Host identified here. To ensure that a host processes all messages IronMail has to deliver, either remove all SMTP entries in the Domain-based routing table, or rename the machine name entries for the SMTP protocol in that table to the machine name or IP address of the Static Host identified here. The **DNS MX Lookup** and **Static Host** options are only valid for messages that are delivered to external domains.
Static Port	If IronMail is configured to deliver all its messages to a Static Host (immediately above), provide in this input field the port number on which IronMail must make the connection.
Highest SMTPO Logging for Troubleshooting	IronMail maintains a log, saved to disk, recording the actions of the SMTPO subsystem. By default, the logging level is set to "Medium"—recording useful information, but not detailed information. During times when maximum information describing how the SMTPO Service processes messages is required, enable this option. Note that logging at this level provides highly detailed information about every email that is processed. In high-volume mail environments (50,000+ messages a day), the daily SMTPO log file can easily grow to 100 MB or more, raising the risk that hard disk space may quickly become consumed. This option should only be enabled for the period of time during which troubleshooting is occurring. Once the need for detailed logging has concluded, this option should be disabled.

SMTPO Service Properties

Field	Description
Messages per Connection	Specify the maximum number of messages IronMail will deliver to a single domain over one connection. For example, if this value is set to “10” and there are 25 messages addressed to Yahoo.com, IronMail will open three connections with Yahoo and send 10 messages in two of the connections, and 5 messages in the third. Note that many servers interpret high numbers of messages on a single connection as Spam and may be configured to drop the connection. The default value of “10” messages per connection is generally acceptable for most environments.
Retry Schedule (secs)	If the receiving server cannot accept a message the first time it is delivered, IronMail can make four additional attempts to deliver it. Enter four numbers, in ascending order, separated by commas. (IronMail requires four values.) Each value represents the number of seconds after the first failed delivery that IronMail should wait before attempting another delivery. IronMail’s default values mean it will make its second attempt 15 minutes after the first failure, its third attempt 4 hours after the original failure, its fourth attempt 24 hours after the original failure, and its final attempt 48 hours after the original failure. After the final failed delivery, IronMail will drop the message. Note, however, that if "Quarantine Undeliverable Messages" is enabled below, IronMail will quarantine undeliverable messages. Administrators have the opportunity to "resend" the quarantined undeliverable messages (with five attempted deliveries each) as many times as they want.
Enable “Warning” Delivery Status Notifications	If this option is enabled, IronMail will send a Delivery Status Notification (DSN) message each time it is unsuccessful in delivering a message. If this option is not enabled, IronMail will only send a DSN after its final delivery attempt was unsuccessful. “Enable DSN to Sender” must be enabled immediately below in order for these “warning” DSN messages to be generated.
Enable DSN to Server	If this option is enabled, IronMail will generate a Delivery Status Notification (DSN) message if it is unable to deliver a message. If enabled and "Enable Warning Delivery Status Notifications" is disabled, the DSN will be generated after the final delivery attempt. If enabled and “Enable ‘Warning’ Delivery Status Notifications” immediately above was also enabled, DSNs will be generated after each failed delivery attempt.

SMTPO Service Properties

Field	Description
Enable DSN to Forwarded Addresses	Delivery Status Notifications may be delivered to one or more individuals in addition to the message sender if this option is enabled and valid email addresses are provided in the input field immediately below.
DSN Forwarded Address	If "Enable DSN to Forwarded Address" is enabled above, DSNs may be delivered to one or more addresses entered in this input field. Enter valid email addresses separated from each other by commas. (Do not enter spaces between commas and subsequent email address.)
Enable DNS Caching	If enabled, IronMail will cache the MX records (or A records) provided by a DNS query for domains to which it delivers messages; the caching will occur right after delivery to the server. The MX record remains in cache until the MX record's time-to-live (TTL) has expired, after which IronMail deletes it. Caching MX records may provide improved performance, because it reduces the need to perform an MX lookup for each mail delivery. If IronMail is unsuccessful in querying for MX records, it will query for A records and try to deliver mail to the A record. It will cache whichever record it delivers to successfully.
DNS Cache Limit	Enter a number (between 100 and 2500) representing the maximum number of MX records IronMail will store in its cache. Every 5 minutes, IronMail will delete MX records whose DNS-specified TTL has expired. When the administrator-defined limit has been reached, IronMail will not allow any additional MX records into its cache until its cleanup process deletes old records. **Note:** SMTPO caches its own DNS records independently. It will continue to draw from its own cache even after DNS changes, until SMTPO is restarted. Restarting flushes out the cache.
TTL for A-records (secs)	While the TTL for MX records is defined by the DNS server, the TTL for A records is administrator-defined. Enter a number (in seconds) representing how long the A records should live in IronMail's cache. (3600, or one hour, is a recommended setting.) IronMail will delete A records whose TTL has expired.

SMTPO Service Properties

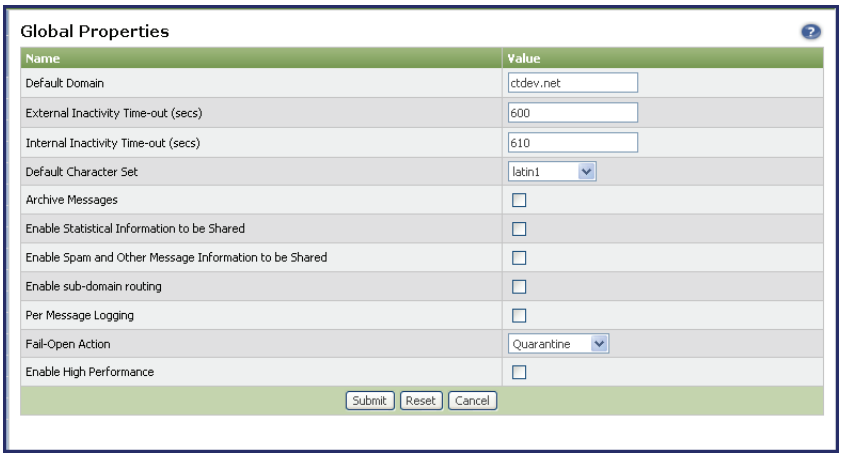
Field	Description
Domain Connection Timeout (secs)	Enter a number (between 300 and 900) representing the maximum number of seconds IronMail may wait for a domain to accept a connection. If a connection cannot be established within this time, IronMail will fall back to the Retry Schedule (above) for additional delivery attempts. (Timeouts may occur if domains are very busy, or a DNS server is unable to respond with the necessary information.)
Quarantine Undeliverable Messages	If a “retry schedule” was configured above, IronMail will make up to five attempts to deliver a message. If this option is not enabled, IronMail drops the message after the fifth attempt. If this option is enabled, IronMail will quarantine undeliverable messages to an SMTPO "Quarantine Queue.” (Access quarantined undeliverable messages at *Queue Manager* > *Outbound Queue* > *Quarantined Messages*.) From the SMTPO Quarantine Queue, administrators may re-send the messages, so that IronMail makes up to another five attempts to deliver it.
Attach Original Message for DSN	Select this option if the original message is to be attached for DSNs generated. If this option is not selected, only headers of the message are attached.
Send FQDN on Helo/Ehlo	If this option is enabled, IronMail will send the Fully Qualified Domain Name when it establishes a connection.

Global Properties

Clicking the Global hyperlink on the last row of the Configure Mail Services table opens a secondary browser window allowing configuration of additional message-delivery options.

The Global Properties screen allows the Administrator to configure properties for IronMail’s mail service. It is important to remember that specific property settings made here will have impact on other IronMail processes. One example is choosing to enable High Performance, or choosing not to enable it.

Protection Management > Mail Firewall > Configure Mail Services > Global



Global Properties

Field	Description
Default Domain	By default, the domain name provided as the "Default Email Domain" during Step 9 of the Installation Wizard is displayed in this input field. You can edit the field by entering the domain name of the server to which IronMail's administrative messages are to be delivered.
External Inactivity Timeout (secs)	Enter a value representing the maximum number of seconds IronMail may wait for external servers (whether inside or outside the network) to respond before closing a connection. It is strongly recommended that the default value of 600 seconds not be changed.
Internal Inactivity Timeout (secs)	Enter a value representing the maximum number of seconds IronMail may wait for its own internal services and subsystems to respond before closing a connection. It is strongly recommended that the default value of 610 not be changed. In any case, this value should be at least 10 seconds greater than the External Inactivity Timeout above.
Default Character Set	Select from the pick list the character set to be used when the character set of a message is unknown. This character set will be used to convert the text to unicode.

Global Properties

Field	Description
Archive Messages	If enabled, IronMail will save all incoming and outgoing messages to disk. At approximately midnight each day, when IronMail generates its Reports and Log Files, it will create a zipped tar archive of the messages and, if configured, transport them to an archive server. Note that messages deleted due to an IronMail process (such as enforcement of a Mail Monitoring or Content Filtering policy) are not archived.
Enable Statistical Information to be Shared	IronMail will securely transfer statistical information about spam and other trends to be used by CipherTrust Research for research purposes only, and to contribute toward increased effectiveness.
Enable Spam and Other Message Information to be Shared	IronMail will securely transfer spam and other message information to be used by CipherTrust Research for research purposes only, and to contribute toward increased effectiveness.
Enable Sub-Domain Routing	If enabled, IronMail will try to resolve sub-domains to a top-level domain identified in the Domain-based routing table (*Mail-Firewall > Mail Routing > Domain-based*). That is, if messages are addressed to “subdomain.domain.com” and “domain.com” is in the routing table, IronMail will deliver it to the internal mail server mapped to that domain. If this option is not enabled, IronMail will only deliver messages to sub-domains if the sub-domains have been specifically added to the routing table.
Per Message Logging	Click the checkbox to cause IronMail to log message details for each message processed. If this function is enabled, the user can view details of messages in IronMail's queues. If it is not enabled, details are not available.
Fail-Open Action	Select an action from the drop down list for the action to be taken on fail-open (when a message fails to open in ST mode). The options are: • Drop message - deletes the message from processing • Quarantine - places the failed message in the Failures Queue • Pass Through - sends the message on through IronMail's processing

Global Properties

Field	Description
Enable High Performance	This option enables or disables IronMail's High Performance capability. Enabling High Performance will improve message processing speed by allowing messages to bypass the MIME Ripper Queue and the Content Extraction Queue. However, this causes the messages to bypass Content Filtering, Attachment Filtering, Whitelisting, Message Stamping, and other IronMail features. High Performance is off by default. Consider the potential ramifications before enabling High Performance.

Mail Routing

IronMail provides several capabilities for routing email. Email addressed to a specific domain may be mapped to a specific internal mail server. An LDAP directory's information may also be used to specify how mail is routed—IronMail will look up the LDAP server information and route the message accordingly. Plus, administrators must explicitly specify which of their internal servers may send messages through IronMail to the outside world. (Unless internal mail servers are identified in the Internal Routing list, IronMail will not deliver their mail to external recipients.)

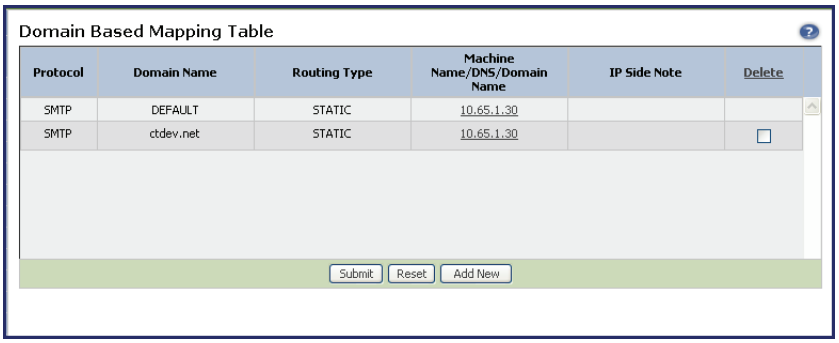
Domain-Based Routing

Specific domains or sub-domains may be mapped to specific internal mail servers. All messages to that domain or sub-domain will be delivered to the specified machine name (internal mail server).

CipherTrust recommends you limit each single IronMail appliance to routing mail to a maximum of 100 internal domains.

To change the default mail server, enter a list of host names or IP addresses separated by commas in the "Machine Name" column for the Default entries for the SMTP protocol. Additional internal mail servers may be added to this list as the number of internal mail servers which IronMail protects, increases.

Protection Management > Mail Firewall > Mail Routing > Domain Based



Domain-Based Routing

Field	Description
Protocol	This column shows the mail service (SMTP) for the domain.
Domain Name	Lists the domain or sub-domain name that IronMail hosts in the corresponding user input field.

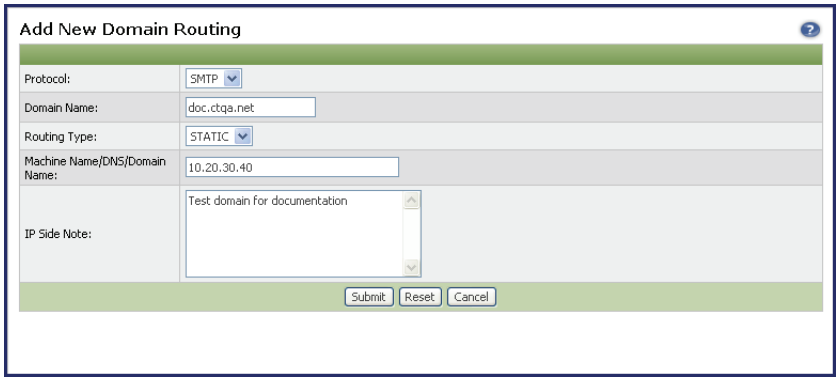
Domain-Based Routing

Field	Description
Routing Type	This column lists the routing type for each domain as it has been configured. See the Add New Domain Routing screen for details.
Machine Name/ DNS/Domain Name	This column shows the fully qualified machine name, IP address or domain name for the mail server responsible for the domain's mail. More than one machine name (or IP address) may exist to provide better routing. "Fail-over" occurs in the order in which the machines are listed in this field.
IP Side Note	This column lists any explanatory or descriptive notes that were configured when someone added a new domain or edited an existing domain.
Delete	To remove mapping of a domain to an internal server, check its **Delete** box and click **Submit**.

Adding a New Routing Domain

Protection Management > Mail Firewall > Mail Routing > Domain Based > Add New

To add a new routing domain to the Domain Based Routing screen, click the **Add New** button at the bottom of the screen. The following screen will open, allowing you to configure the new domain.



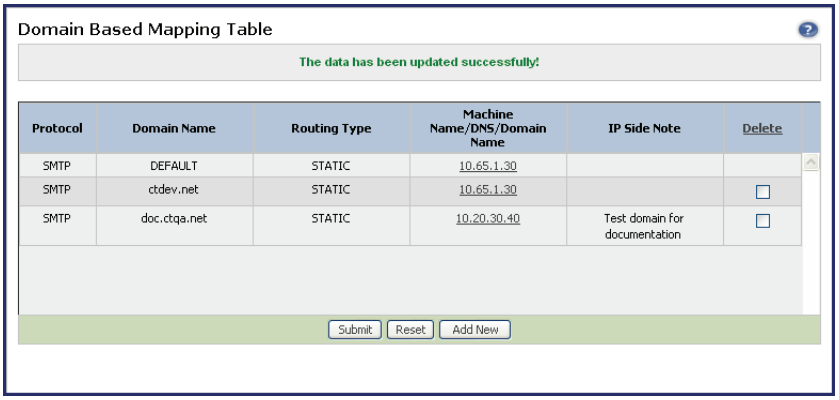
Adding a New Routing Domain

Field	Description
Protocol	From the list, select the mail service. For IronMail Edge, SMTP is the only selectable option.
Domain Name	Enter the domain or sub-domain name that IronMail will use to host the domain.
Routing Type	Select the routing type for the domain from the pick list. For IronMail Edge, the routing type is always Static.

Adding a New Routing Domain

Field	Description
Machine Name/ DNS/Domain Name	Enter the IP address of the mail server responsible for the domain's mail.
IP Side Note	Enter any explanatory or descriptive notes that should appear in the mapping table.

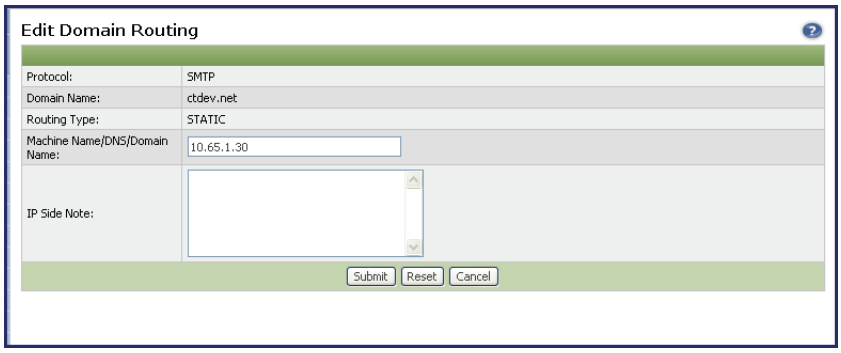
When the information is complete, click Submit. the Domain Based Routing screen will update as shown below.



Editing an Existing Domain

Protection Management > Mail Firewall > Mail Routing > Domain Based > Domain hyperlink

To edit the configuration of an existing routing domain, click the hyperlink for that domain, which appears in the Machine Name/DNS/ Domain Name column on the Domain Based Routing screen. An edit screen will open, as shown below.



This screen allows you to view the existing information about the domain you selected, and to edit some of the fields.

Editing a Routing Domain

Field	Description
Protocol	This field contains the protocol for this domain. This field is not editable.
Domain Name	This field contains the domain name or subdomain for this routing configuration. This field is not editable.
Routing Type	This field shows the routing type for the domain. The field is not editable.
Machine Name/ DNS/Domain Name	Enter the IP address of the mail server responsible for the domain's mail. Unless Alternate MX has been selected as the routing type, more than one IP address may be added to provide better routing. Separate the machine names or IP addresses with commas and *without spaces* between the commas and the subsequent name or IP address. "Fail-over" occurs in the order in which the machines are listed in this field. If Alternate MX is selected, only one IP address may be added.
IP Side Note	Enter any explanatory or descriptive notes that should appear in the mapping table.

When you click Submit, the edited domain information will appear in the Domain Based Routing screen.

Mail Intrusion Detection Service

The Mail-IDS (Intrusion Detection System) program area provides a variety of tools designed to detect network attacks against the email gateway, as well as a tool to test for weaknesses or vulnerabilities in specific internal mail servers. IronMail will automatically generate alerts for certain types of network attacks, notifying administrators immediately by email, pager, or SNMP that an event has occurred. For all attack events, IronMail will log their occurrence so they may be viewed in IronMail's log files and daily reports, and in IronMail's Dashboard. Administrators, therefore, should configure IronMail's Alert Manager to send to them alerts that the Mail-IDS services generate. And administrators should routinely monitor IronMail's Dashboard and Mail-IDS Report throughout each day.

In this chapter

In this chapter you will find information about the following topics:

- Application Level Protection
  - Denial of Service Protection
  - Configuring Application Level Protection
- Network Level Protection
  - The Analysis Console
  - Configuring Network Level Protection
  - Signature Manager
- System Level Protection
  - Program Integrity
  - File System Integrity

Application Level Protection

IronMail offers tools designed to protect against attacks directed at email applications.

Denial of Service Protection

IronMail automatically monitors and logs repeated connections to a specific port from the same IP address. If an administrator-defined number of connections to a single port are attempted within a specified period of time, IronMail assumes that it is a Denial of Service (DoS) attack and will drop all incoming connections to that port from that address for a user-specified amount of time. The Denial of Service

threshold (a specified number of connections within a defined length of time) is set in *Protection Manager > Mail-IDS > Application Level > Configure* with the "Denial of Service Count" and "Denial of Service Window" parameters.

Protection Manager > Mail IDS > Application Level > DoS Protection

The Denial of Service Protection table lists a summary of all DoS attacks recorded since IronMail's cleanup process deleted the DoS data; each time this page is refreshed, the data is updated with the most recent attacks. The information here may also be viewed in the daily Mail-IDS Report created at approximately midnight each day. Note, however, that whereas IronMail's Denial of Service window may show several days' (or more) worth of information, the daily Mail-IDS report will only show 24 hours worth of data.)

Denial of Service Protection

Field	Description
Service	This column reports which of the IronMail services encountered the Denial of Service (DoS) attack: POP3/POP3S, IMAP4/IMAP4S, or SMTPI/SMTPIS.
Source IP	This column reports the IP address from which the DoS attack originated. Consider adding the IP address to IronMail's Local Deny List to block all further SMTP connections from that source.
Date	This column reports the timestamp when the DoS threshold was reached. If the same IP address generates another DoS later in the day, the previous timestamp is updated to reflect the time of the new attack.

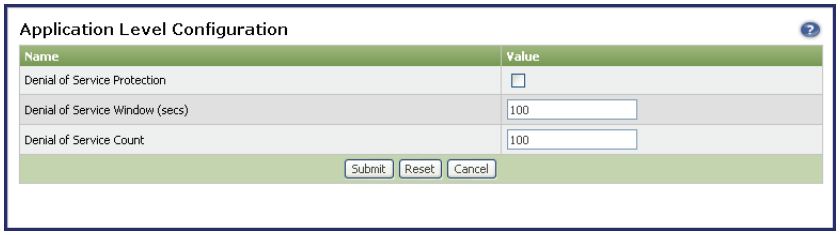
Denial of Service Protection

Field	Description
Connections	This column reports the number of connections that were dropped after the DoS threshold was reached. Remember that IronMail will drop further connections only for the length of time specified as the "Denial of Service Window." If multiple DoS attacks from the same IP address are detected throughout the day, IronMail will display in this column a running total of dropped connections that occurred during the separate "drop windows" that follow each time a threshold was reached.

Configuring Application Level Protection

Use the values entered in this window to set the threshold for application-level attacks aimed at the internal network.

Protection Manager > Mail IDS > Application Level > Configure



Configuring Application Level Protection

Field	Description
Denial of Service Protection	If Denial of Service Protection is enabled, IronMail will monitor all TCP connections to all email ports on which it listens (25, 110, 143, etc.), and block future connections for any IP address that exceeds the Denial of Service threshold (created with the two values that appear immediately below). IronMail will discontinue accepting connections from the offending IP address for the length of time specified in the "Denial of Service Window" below. Once that length of time passes, IronMail will again begin allowing connections from that source IP address. Ensure that IronMail's Alert Manager is configured to send Warning alerts for the SMTPI Service so an administrator may immediately add the offending IP address to IronMail's Local Deny List, after which IronMail will no longer accept connections from that IP address. Be aware that in some environments, applications legitimately make high numbers of connections which IronMail may interpret as a Denial of Service attack. Consult with the network administrator before setting this value.
Denial of Service Window (secs)	Enter a number, from 1 to 65,535, representing the length of time in seconds in which connections from a single IP address will be accepted after which a Denial of Service attack is assumed. (The default value of "100" is generally acceptable.) If IronMail receives the number of connections specified in the "Count" field above within this "window," further connections from the source IP address will be dropped. IronMail also uses this value as the length of time IronMail rejects further connections. Once the time has lapsed, IronMail again begins accepting connections from the source IP address.
Denial of Service Count	Enter a number, from 1 to 65,535, representing the maximum number of allowed connections to a single port before which a Denial of Service attack is assumed. (The default value of "100" is generally an acceptable value.) When a single IP address generates the specified number of connections within the time frame indicated below, a Denial of Service attack is assumed and further connections from that source will be dropped.

Network Level Protection

IronMail provides a Network IDS engine that examines in real-time all network traffic flowing through email ports (ports 25, 110, 465, etc.). Viewable through IronMail's Analysis Console, it begins creating a log whenever data or network packets match known "signatures" for attempts at hacking. Once detected, the entire stream of packets is captured for analysis.

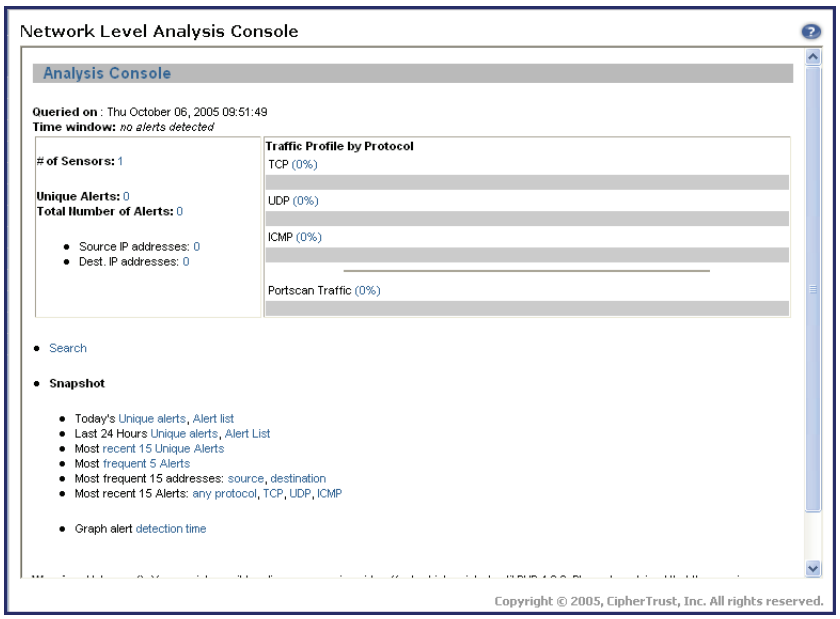
For those administrators who actively respond to network attacks and create rules to block future occurrences, the Analysis Console provides visibility into network traffic at the TCP level. It is assumed that users taking advantage of this tool are already experienced and knowledgeable in its use.

Analysis Console

The Analysis Console displays a static report—information captured up to the moment the Analysis Console was opened. Re-clicking the Analysis Console hyperlink in the left navigation frame refreshes the report with the latest information.

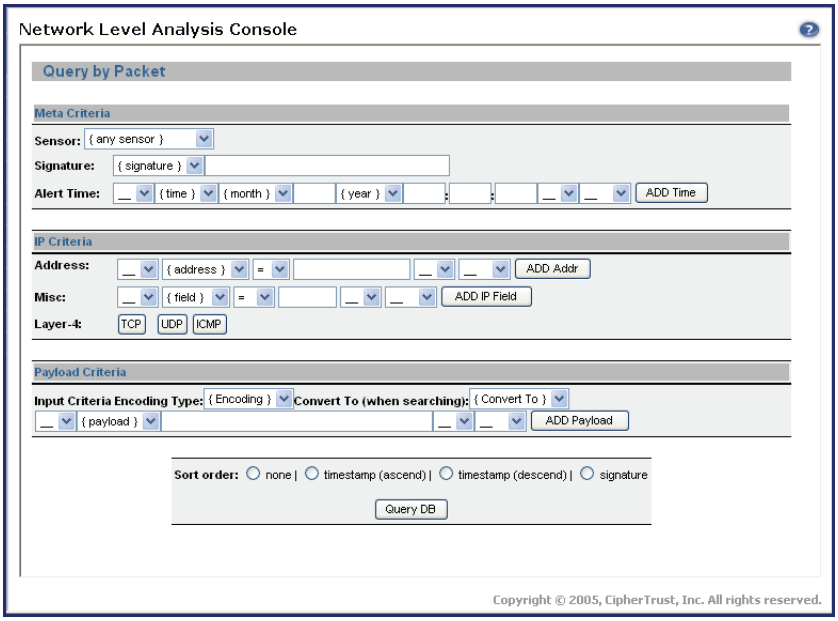
The Analysis Console reports "Alerts"—instances of TCP, UDP, and IMCP traffic that matched an attack signature for which Network IDS was scanning. Network IDS uses the attack signatures specified in *Protection Manager > Mail IDS >Network Level > Signature Manager* to identify these attacks.

Protection Manager > Mail IDS > Network Level > Analysis Console


Network Level Analysis Console
Analysis Console
Queried on : Thu October 06, 2005 09:51:49
Time window: no alerts detected
# of Sensors: 1
Unique Alerts: 0
Total Number of Alerts: 0
Source IP addresses: 0
Dest. IP addresses: 0
Traffic Profile by Protocol
TCP (0%)
UDP (0%)
ICMP (0%)
Portscan Traffic (0%)
Search
Snapshot
Today's Unique alerts, Alert list
Last 24 Hours Unique alerts, Alert List
Most recent 15 Unique Alerts
Most frequent 5 Alerts
Most frequent 15 addresses: source, destination
Most recent 15 Alerts: any protocol, TCP, UDP, ICMP
Graph alert detection time
Copyright © 2005, CipherTrust, Inc. All rights reserved.

Any text appearing in blue is a hyperlink that reveals additional information about the events. For example, clicking the link for Today's Unique Alerts or Alert List will open an Alert Listing screen. Clicking

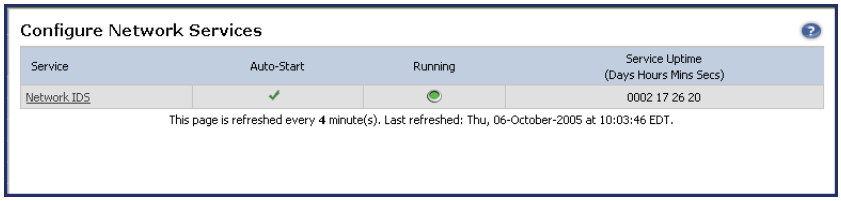
the Search hyperlink allows you to construct detailed queries against the information stored in the Analysis Console.


Network Level Analysis Console
Query by Packet
Meta Criteria
Sensor: { any sensor }
Signature: { signature }
Alert Time: { time } { month } { year } ADD Time
IP Criteria
Address: { address } ADD Addr
Misc: { field } ADD IP Field
Layer-4: TCP UDP ICMP
Payload Criteria
Input Criteria Encoding Type: { Encoding } Convert To (when searching): { Convert To }
{ payload } ADD Payload
Sort order: none | timestamp (ascend) | timestamp (descend) | signature
Query DB
Copyright © 2005, CipherTrust, Inc. All rights reserved.

Configuring Network Level Protection

To configure network level protection, navigate to the Configure Network Services

Protection Manager > Mail IDS > Network Level > Configure


Configure Network Services
Service
Auto-Start
Running
Service Uptime (Days Hours Mins Secs)
Network IDS
0002 17 26 20
This page is refreshed every 4 minute(s). Last refreshed: Thu, 06-October-2005 at 10:03:46 EDT.

The screen displays the current status of Network IDS services.

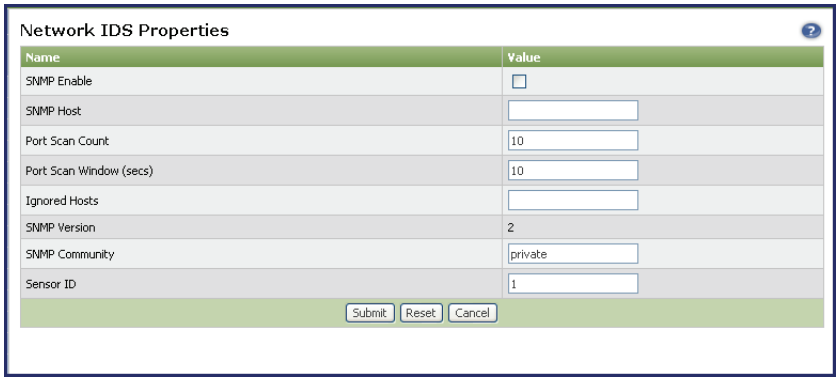
Configuring Network Services

Field	Description
Service	The first column contains the service name, which is Network IDS.
Auto-Start	A check mark in this column indicates the service is configured to be restarted automatically if Health Monitor finds it has stopped. A red X indicates the service will not be restarted. Clicking the icon toggles auto-start on and off.

Configuring Network Services

Field	Description
Running	A green light icon in this column indicates the service is currently running. A red icon indicates it is not running. Clicking the icon will start or stop the service.
Service Uptime	This column shows the elapsed time in days, hours, minutes and seconds the service has been running since it was last started.

The service name is a hyperlink that opens the Network IDS Properties screen.



Network IDS Properties

Field	Description
SNMP Enable	Select the **SNMP Enable** check box to allow IronMail's Analysis Console to deliver its network events as traps to a network SNMP console. Note that enabling SNMP here is independent of enabling SNMP in IronMail's Alert Manager. That is, enabling SNMP traps as an alert mechanism for IronMail's alerts does not automatically allow the delivery of Analysis Console traps.
SNMP Host	Enter the hostname of the SNMP server.

Network IDS Properties

Field	Description
Port Scan Count	While the Denial of Service configuration establishes a threshold for connections from a single IP address, that threshold is specific to TCP connections to a single port. This Port Scan threshold counts any TCP connection to any port that originates from the same IP address. Enter a maximum number of allowed connections, from 1 to 65,535, in the “Count” field. When a single IP address generates the specified number of connections within the time frame indicated below, the connection will be logged as an Analysis Console “event.” In addition to detecting TCP connections, Analysis Console detects stealth scans (precursor or reconnaissance activity prior to an attack). A single instance of a NULL, FIN, SYNFIN, or XMAS-type stealth scan will be logged as an Analysis Console “event.”
Port Scan Window (secs)	Enter a number of seconds, from 1 to 65,535, in the “Port Scan Window” field indicating the “window” in which connections may occur. When a single IP address generates the specified number of connections within the time frame indicated here, the connection will be logged as an Analysis Console “event.”
Ignored Hosts	Enter the IP address for any host IronMail should ignore. (These hosts are allowed to scan IronMail as much and as often as they like.) Use commas to separate multiple IP addresses from each other.
SNMP Version	Enter the SNMP version number. Note that IronMail only supports SNMP version 2c. When entering the SNMP version number in this input field, however, only enter the numeral “2.”
SNMP Community	By default, when SNMP is installed, two default "communities" are created: "Private" and "Public." The SNMP administrators should have created one or more idiosyncratic community names for the services SNMP is monitoring. Enter that community name in this input field.
Sensor ID	Enter a unique ID number for the sensor.

When the information is correctly entered, click **Submit** to save the configuration.

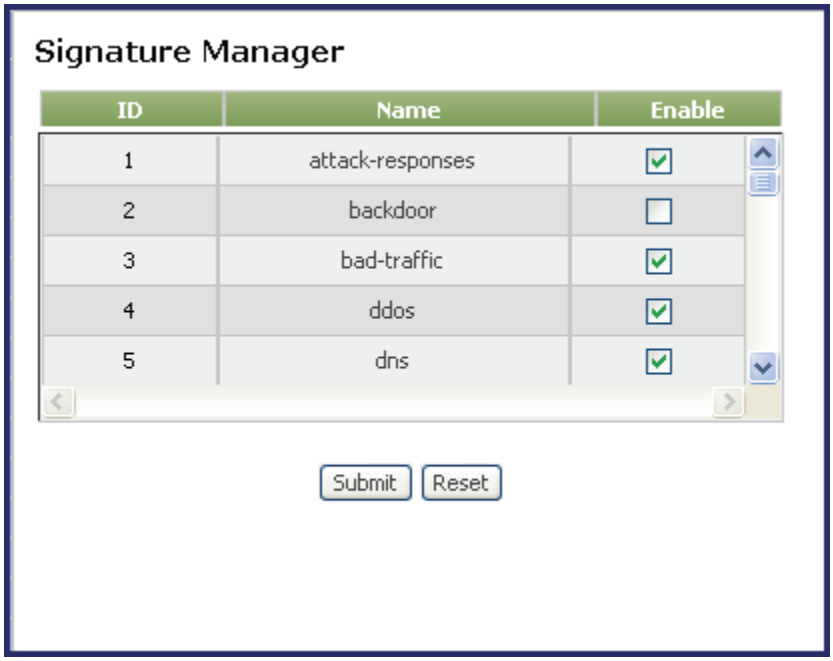
If the Analysis Console is enabled, administrators should monitor the number of generated events on a regular basis—one or more times a day if necessary. High numbers of events stored in IronMail's database can begin to adversely affect overall IronMail performance. If more than 100,000 IDS events are recorded and stored to disk before Iron-

Mail's Cleanup Schedule deletes old Mail-IDS data files, lower the "age" at which IronMail should delete data. That is, if IronMail's Cleanup Schedule is configured to wake up every 24 hours and delete files that are 48 hours old, consider re-configuring it to wake up every 12 hours and delete data that is 24 hours old.

Signature Manager

The Network IDS Service compares packet information against over 1300 known attack signatures. The Signature Manager table displays a list of broad categories of attack threats.

Protection Manager > Mail IDS > Network Level > Signature Manager



Signature Manager

Field	Description
ID	This column indicates the ID number, used internally by IronMail, of the category of attack signatures.

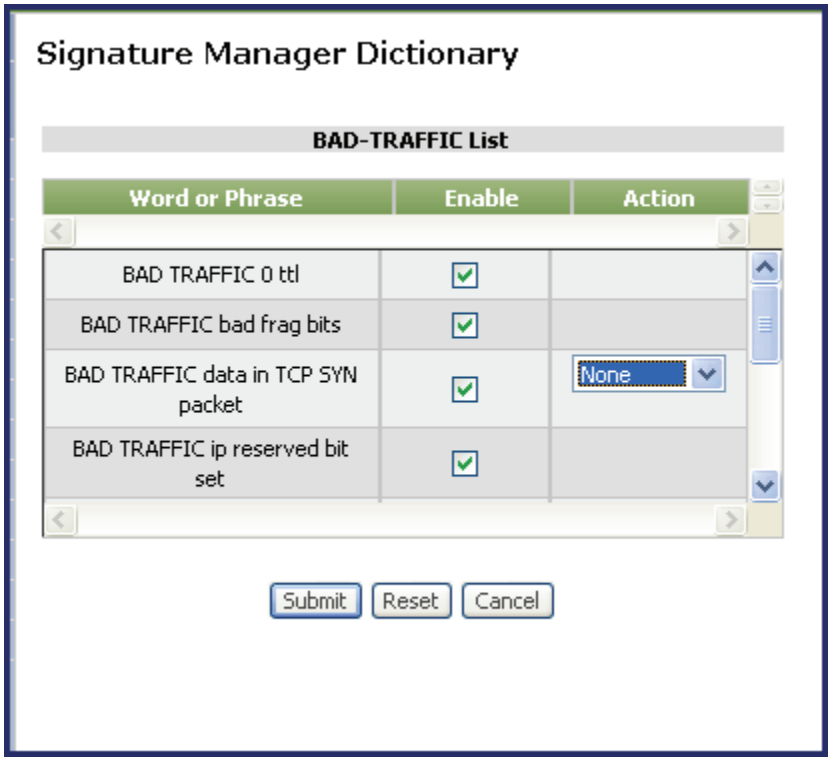
Signature Manager

Field	Description
Name	This column displays the “category name” of a set of attack signatures. The category name is indicative of the type of attacks they identify. For example, “ddos” is a category containing signatures that identify a variety of distributed denial of service attacks, and “web-cgi” is a category of signatures related to attacks against web-based CGI applications and scripts. The category name is also a hyperlink that opens in a secondary browser window a list of all the individual signatures within that category.
Enable	The **Enable** check boxes for each category allow the administrator to decide whether or not to include an entire category of signatures in IronMail’s real-time analysis of email traffic.

Signature Dictionary

Protection Manager > Mail IDS > Network Level > Signature Manager > Dictionary

Click an attack category’s hyperlink to open a list all the individual attack signatures within that category.



Signature Dictionary

Field	Description
Signature	The signature's category name appears at the top of the screen.
Word or Phrase	This column identifies a "friendly" name of the attack signature.
Enable	Select or deselect a signature's **Enable** check box to indicate whether or not IronMail should include it in its real-time analysis of email traffic.
Action	IronMail is capable of actively responding to some attacks, typically by resetting the TCP connection. If an action is possible, the Action column will display a pick list allowing the choice of either "TCP Reset" or "ICMP Reset." Leave the action set to "None" if IronMail should not reset the connection if an attack is detected. Only administrators familiar with firewall rules should enable actions for attack signatures. IronMail will blindly reset connections when it encounters packet data it thinks matches attack signatures, whether the data stream is valid or not. And because IronMail has been specifically "hardened," and thus immune from these attacks, setting an action may be moot.

Signature Updates

Note that CipherTrust regularly updates its database of attack signatures; updated signatures may be automatically downloaded and installed on individual IronMail's. However, customers must have purchased a Mail-IDS Updates license to benefit from these updates.

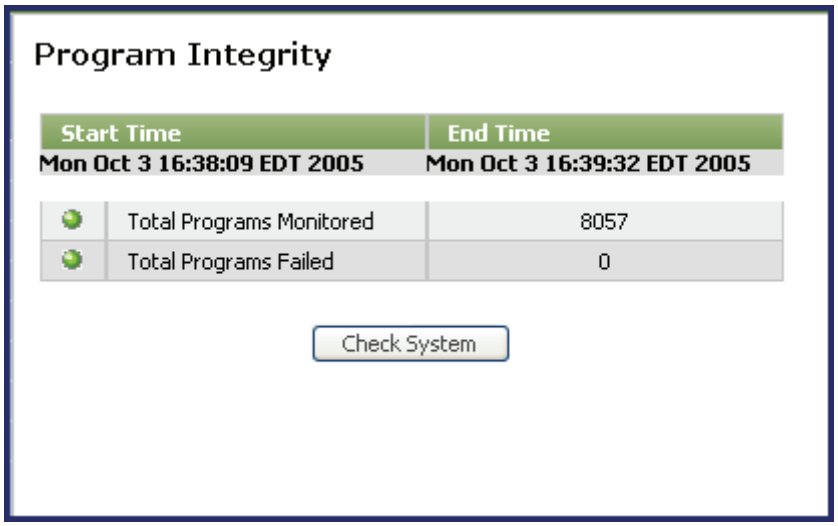
System Level Protection

IronMail is foremost an appliance to protect the internal mail servers sitting behind it. An integral component of its security, however, is ensuring that it (that is, IronMail) has not been compromised by an attacker. The Program Monitor and File Monitor services, therefore, check IronMail's program files and filesystem in order to detect whether or not an attempt has been made to alter code in any of its files, or if an attempt was made to insert Trojan horses or delete important system files. The first time IronMail restarts after the Initial Configuration Wizard is run, its Program Monitor and File Monitor test the system in order to build an initial database of IronMail's file set and file system. Thereafter, these two services run nightly, immediately before the Mail-IDS log is generated. Administrators may run File Monitor and Program Monitor "on demand" at any time by clicking Check System in their respective windows.

Program Integrity

Every night, at approximately midnight, IronMail examines every executable file within its scope to verify that they have not been altered. The Program Integrity page displays how many files were scanned, and the number of files that failed its test, i.e. are now different from their original version. To manually run IronMail's Program Monitoring in-between scheduled sessions, click Check System. It will take a little less than a minute to run its tests.

Protection Manager > Mail IDS > System Level > Program Integrity



After clicking **Check System** IronMail will check, approximately every 10 seconds, if Program Integrity Monitor has finished its tests, then refresh the page with the results. If Program Integrity Monitor ever reports that a single file failed, contact CipherTrust Technical Support immediately.

The information available here may also be viewed in IronMail's Dashboard and the Mail-IDS Report that is created daily.

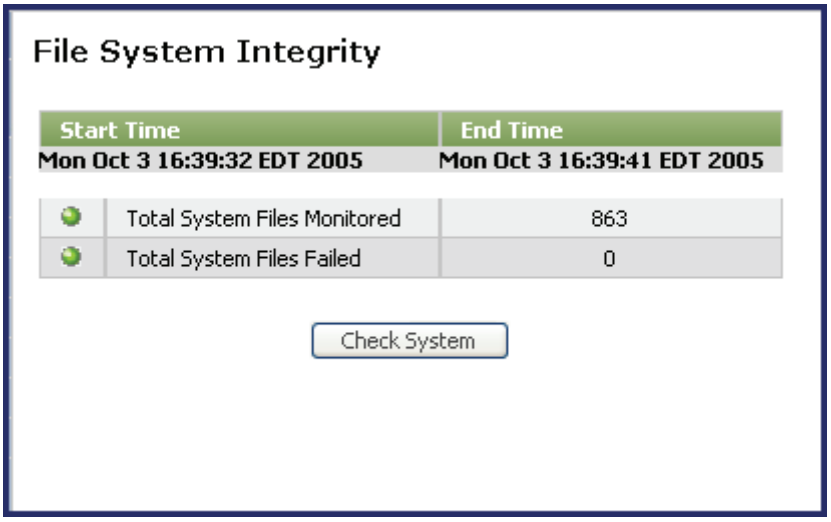
Program Integrity

Field	Description
Start Time	The date and specific time the test began appears in this field.
End Time	The date and specific time the test ended appears in this field.
Total Programs Monitored	The total number of programs checked by the Program Integrity test shows here.
Total Programs Failed	The number of programs, if any, that failed the integrity test shows here.
Check System	This button allows you to run a Program Integrity check at will, should circumstances warrant it.

File System Integrity

Similarly, every night at approximately midnight, IronMail examines its internal filesystem to ensure that no non-IronMail-generated files have been created on it or that none of IronMail's files were deleted. To manually run IronMail's File Monitoring in-between scheduled sessions, click **Check System**. It will take a little less than a minute to run its tests.

Protection Manager > Mail IDS > System Level > File System Integrity



Approximately every 10 seconds, IronMail will check if Filesystem Integrity Monitor has finished its tests, and then refresh the page with

the results. If Filesystem Integrity Monitor ever reports that a single file failed, contact CipherTrust Technical Support immediately.

File System Integrity

Field	Description
Start Time	The date and specific time the test began appears in this field.
End Time	The date and specific time the test ended appears in this field.
Total System Files Monitored	The total number of files checked by the File System Integrity test shows here.
Total System Files Failed	The number of files, if any, that failed the integrity test shows here.
Check System	This button allows you to run a File System Integrity check at will, should circumstances warrant it.

V: Reporting

Introduction

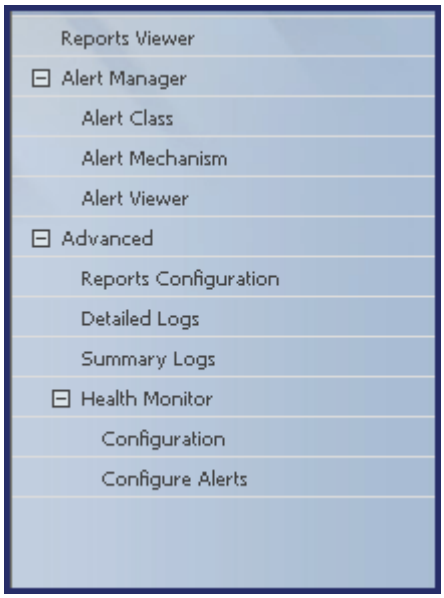
IronMail's reporting and monitoring tools are what make IronMail such a robust and usable appliance. Through its logs, administrators can determine exactly which IronMail processes examined a message—indeed, whether or not IronMail even received the message. When an IronMail policy acts upon a message, the reports and logs will describe exactly what condition of the policy caused IronMail to act.

In addition to reporting on IronMail's internal message-processing, this program area also contains "Health Monitor"—a subsystem that examines all other core application subsystems, as well as hardware, to ensure that the appliance is operating as designed. And on the belief that IronMail cannot truly protect an enterprise's email system if the appliance, itself, is vulnerable, an Alert Manager can be configured to generate email, pager, or SNMP trap alerts to the administrator whenever Health Monitor detects that IronMail is not performing as designed.

In this section

In this section, you will find the following chapters:

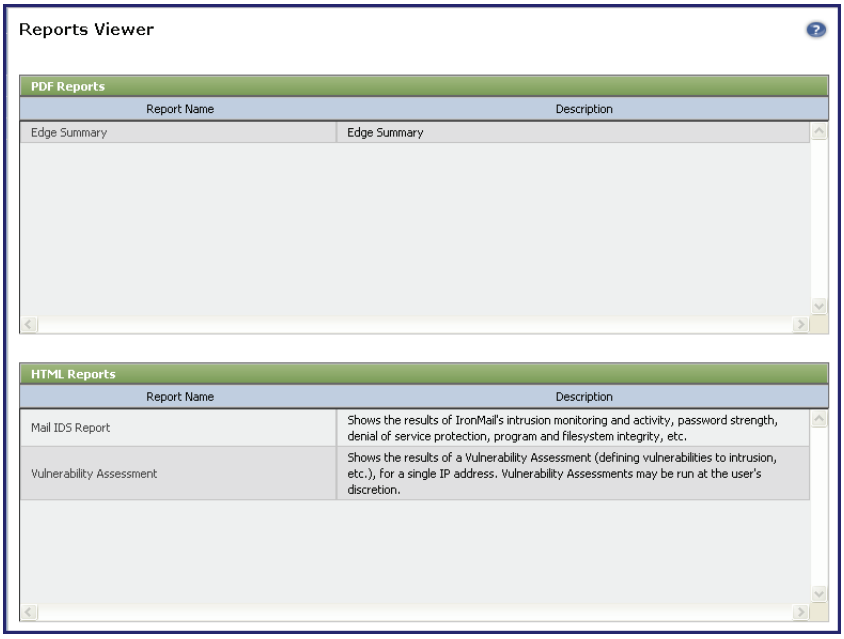
- Chapter 7: Alerts Manager
- Chapter 8: Health Monitor
- Chapter 9: Advanced Reporting



The Reports Viewer

When you log into the Reporting program area, the opening screen is the Reports Viewer. This screen lists IronMail's reports and briefly describes them. Each Report Name is a hyperlink that opens a more detailed page about the specific report, revealing recent history and allowing you to review or transfer reports.

Login > Reporting


Reports Viewer
PDF Reports
Report Name
Description
Edge Summary
Edge Summary
HTML Reports
Report Name
Description
Mail IDS Report
Shows the results of IronMail's intrusion monitoring and activity, password strength, denial of service protection, program and filesystem integrity, etc.
Vulnerability Assessment
Shows the results of a Vulnerability Assessment (defining vulnerabilities to intrusion, etc.), for a single IP address. Vulnerability Assessments may be run at the user's discretion.

The report lists are scrollable, allowing you to see a complete listing of all IronMail reports. Clicking any report hyperlink reveals details.

Alert Manager

IronMail continuously monitors its core subsystems, as well as its ability to communicate with internal mail servers. If any part of IronMail's functionality fails to perform as designed, IronMail will generate an "alert." The alerts, by themselves, don't do anything. Rather, the Alert Manager—which processes all IronMail-generated alerts—must be configured to send them to an administrator.

IronMail's alert management is configured on the basis of two groups:

- **IronMail subsystems:** The IronMail application is comprised of core subsystems. Each one is designed to generate alerts when anomalous conditions are experienced. Administrators will create logical groupings of these subsystems.
- **Alert Levels:** IronMail is designed to look for specific types of problems—such as a subsystem stopping unexpectedly, or restarting after it was stopped. There are a finite number of anomalies that IronMail can report on (see the table of alerts). Each anomaly may be assigned one of seven "alert levels" according to the degree of criticality of the problem.

IronMail administrators will create an alert mechanism (email, pager, SNMP trap) for any or all of the "alert levels," for each grouping of subsystem they have created.

In this chapter

In this chapter you will find information about the following topics:

- Alert Levels
- Alert Classes
- Alert Mechanisms
- The Alert Viewer

Alert Levels

The possible alerts IronMail can send are as follows:.

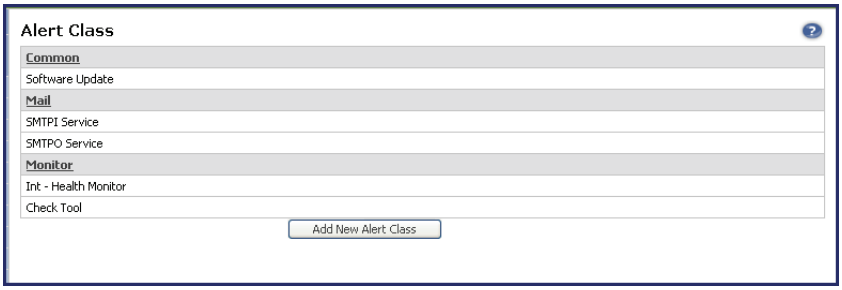
- **Information:** This alert is for information only. No problem exists. It reports, for example, that an SNMP heartbeat has been sent.
- **Notification:** This alert is slightly more important than "information." It reports information about an IronMail process or service. For example, it reports that an anti-virus update has been received.

- **Warning:** A warning should "get your attention." It implies that administrative action is warranted. For example, IronMail generates a warning when a Denial of Service attack has been detected.
- **Error:** An error is serious. IronMail generates error messages when a single process is not performing as intended. For example, it generates an error alert if it detects that IronMail's Content Filtering Queue stops processing messages.
- **Critical:** A critical alert is even more serious. IronMail generates this alert when an error affects the entire appliance. It reports, for example, when IronMail cannot reach a DNS server.
- **Shutdown**: This alert is reserved for future functionality.
- **Restart:** This alert is reserved for future functionality.

Alert Class

The Alert Class screen allows the Administrator to define groups of related services. Groups may be added, edited and deleted, and services may be assigned and reassigned to groups through this functionality.

Reporting > Alert Manager > Alert Class



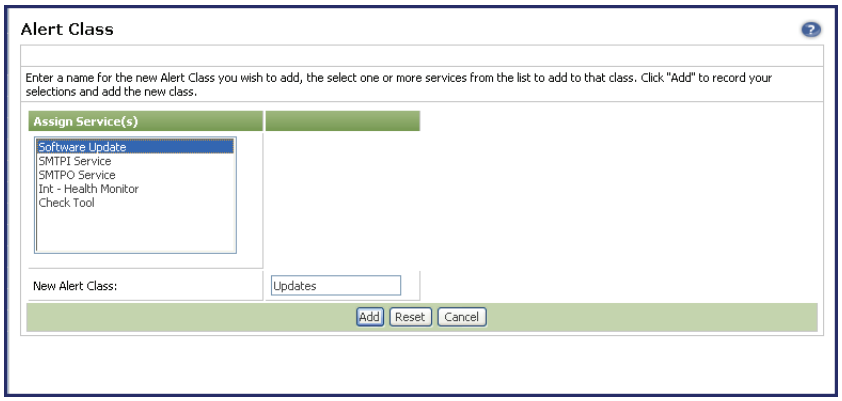
By default, IronMail starts with one logical grouping, or "class," of subsystems: SNMP. Administrators may create any logical grouping of services that serves their needs. Individual subsystems may be moved from one grouping or "class" to another or deleted altogether. The purpose of creating classes of subsystems is to be "granular" in terms of which alert notifications are received, as will be explained below. When the classes have been added, Alert Levels may be configured for them using the Alert Mechanism function.

If a subsystem is deleted from a group and not added to another, IronMail will automatically create a class named "Common" and place the unused subsystem there. Alerts that might be generated by a subsystem in the Common class are not delivered to an administrator unless an alert mechanism for the Common class is created.

Adding an Alert Class

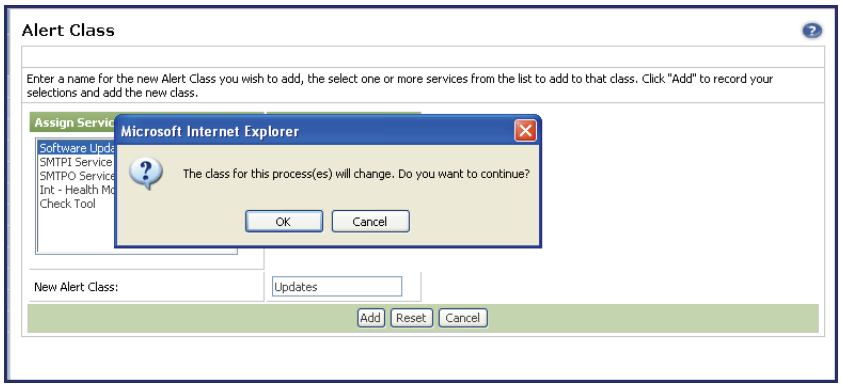
Adding a new class begins when the Administrator clicks the Add New Alert Class button and the bottom of the Alert Class Screen. The following screen opens.

Reporting > Alert Manager > Alert Class > Add New Alert Class

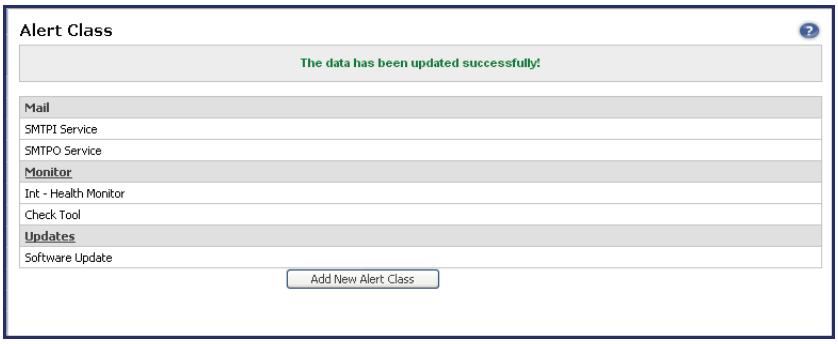

Alert Class
Enter a name for the new Alert Class you wish to add, the select one or more services from the list to add to that class. Click "Add" to record your selections and add the new class.
Assign Service(s)
Software Update
SMTPI Service
SMTPO Service
Int - Health Monitor
Check Tool
New Alert Class:
Updates
Add
Reset
Cancel

To add the new class, enter the name for the class in the New Alert Class data field, then select from the scrolling list one or more services to be included in the class. Click **Add** when the selection is finished.

The following warning screen will appear.


Alert Class
Enter a name for the new Alert Class you wish to add, the select one or more services from the list to add to that class. Click "Add" to record your selections and add the new class.
Assign Servic
Software Upda
SMTPI Service
SMTPO Service
Int - Health Mo
Check Tool
Microsoft Internet Explorer
The class for this process(es) will change. Do you want to continue?
OK
Cancel
New Alert Class:
Updates
Add
Reset
Cancel

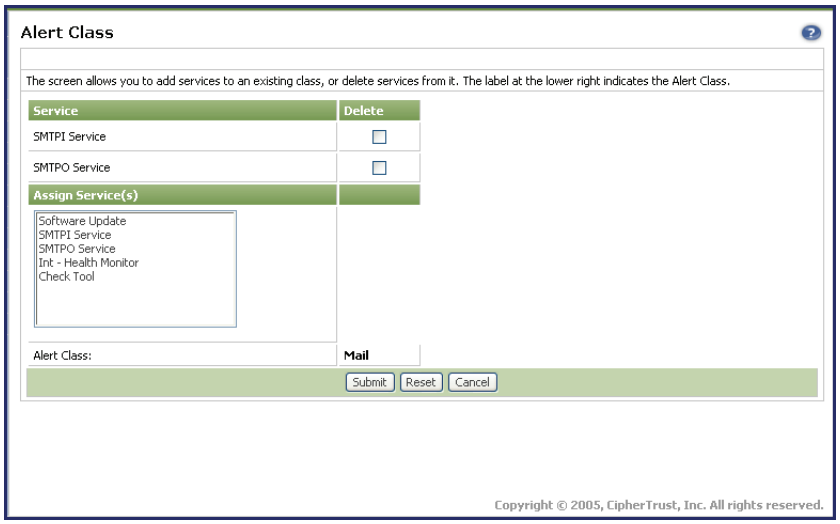
If you want to assign the relevant service or services to the new class, click **OK**. The screen will refresh.



You can repeat the process until you have the set of classes necessary for your system.

Editing an Alert Class

You may also edit an existing class. Begin by clicking class name hyperlink. The following screen displays.



Editing an Alert Class

Field	Description
Service	This column shows the current list of subsystems assigned to this class.
Delete	Checking the Delete check box for any subsystem will delete it from the class. The subsystem will go back to the default (Common) class.
Assign Services	The column displays all services select one or more of them to be added to the class.
Alert Class	The name of the Alert Class being edited appears at the bottom of the screen. The name is not editable.

When you have completed the desired changes, click **Submit**. The Alert Class screen will refresh, showing your new configuration.

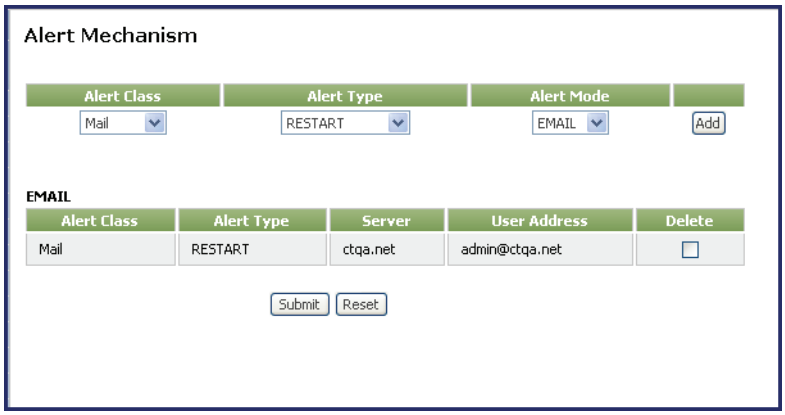
You can delete an entire class from the list by checking Delete for all the services and clicking **Submit**. A confirmation alert will appear; click **OK** to complete the deletion. All the services will go back to the default (Common) class.

After the Alert Classes have been created, create the Alert Mechanism for each class to determine how alerts will be delivered.

Alert Mechanisms

The Alert Mechanism page is where Alert Manager is configured to send alerts to the administrator by email, pager, or SNMP traps. An alert mechanism must be configured for each level of alert, and for each group or "class" of IronMail subsystems for which the administrator wants notification. For example, if administrators want to be notified whenever the SMTPO Service stops performing (reported as an "Error" alert by IronMail), an "Error" email, pager, or SNMP alert mechanism must be configured for the class that contains the SMTPO Service. Conversely, if alert mechanisms for "Information" alerts are not created for a particular class, no "Information" alerts for any subsystem within that class will be sent to the administrator.

Reporting > Alert Manager > Alert Mechanism



The Alert Mechanism page contains three pick lists allowing configuration of alerts notifications, and displays a table of all configured alerts

Alert Mechanism

Field	Description
Alert Class	The Alert Class pick list contains the names of all classes of subsystems that have been created. (IronMail creates a default "Common" class to contain unused subsystems.) Select a class from the list, and then select related values in the Alert Type and Notification Type pick lists.

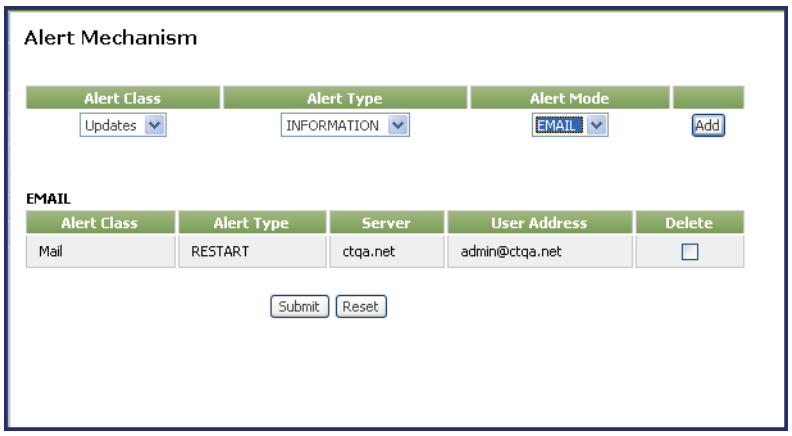
Alert Mechanism

Field	Description
Alert Type	The pick list contains the seven Alert Levels that IronMail can generate. Select an alert level from the list. Options are: • **Information** • **Notification** • **Warning** • **Error** • **Critical** • **Shutdown** • Restart For each class, select a level or type of alert as well as an Alert Mode.
Alert Mode	The pick list offers three choices for alert delivery: • **Email** - one or more email addresses will be required. • **Pager** - requires the *host name* of the server that processes pager messaging, plus one or more pager addresses. (Multiple pager addresses must be separated from each other with commas. Do not enter spaces between commas and subsequent addresses.) • **SNMP** - requires the host name of the SNMP server, the port number through which communication with it occurs, and the version number of the SNMP application.
Add	Click this button to set up a new Alert Mechanism.
Configured alert mechanisms	*The table in the lower part of the screen contains information about all the existing alert mechanisms.*
Alert Class	This column shows by name all alert classes for which alert mechanisms have been defined.
Alert Type	This column lists the alert type associated with each class.
Server	This column is populated with the server names where the recipient type resides.
User Address	The user address that is to receive the alert shows here.
Delete	Clicking the check box and then clicking **Submit** will cause the alert mechanism to be deleted from the list.

Adding an Alert Mechanism

To add a new alert mechanism, use the pick lists at the top of the screen. Select the class, the type of alert, and the alert mode.

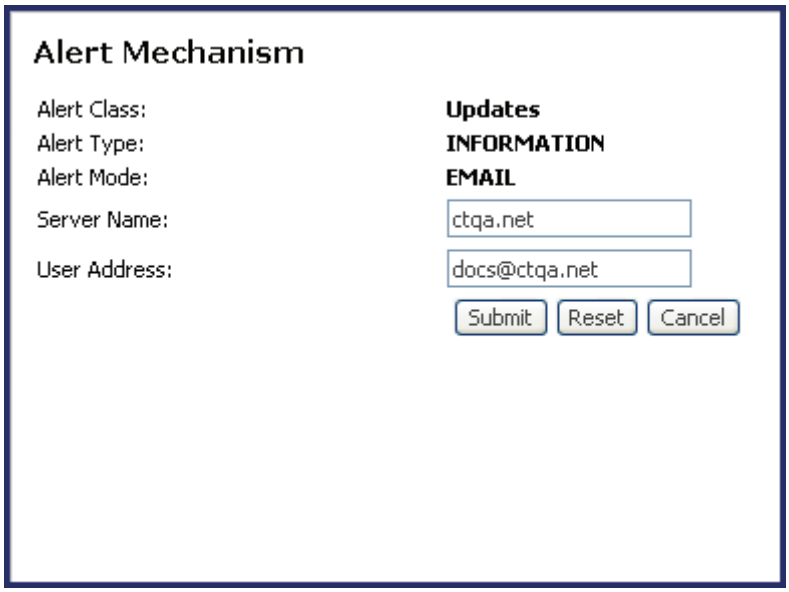
Reporting > Alert Manager > Alert Mechanism > Add



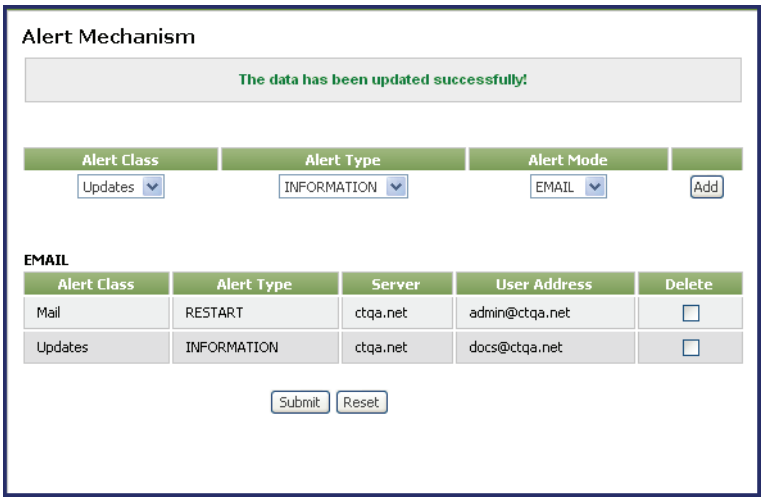
When you click add, the appropriate secondary screen will open.

Adding an Email Mechanism

The screen below appears if you selected Email as your Alert Mode.



For an Email notification, you must supply the server name where the pager address is located, and you must enter the user address. When you click **Submit**, the main Alert Mechanism screen refreshes.



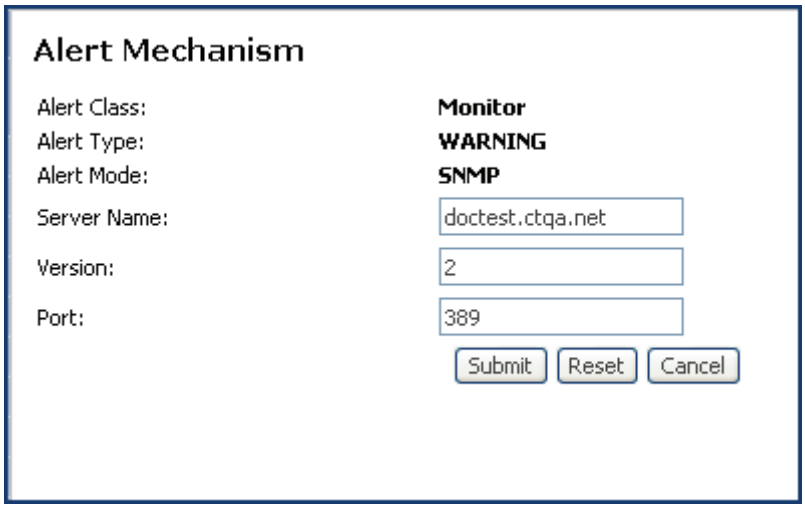
Adding a Pager Alert Mechanism

The following screen is used for Pager alert mechanisms.

As with the Email alert mechanisms, you must supply the server name and the user address.

Adding an SNMP Alert Mechanism

The following screen is used to configure an SNMP alert mechanism.

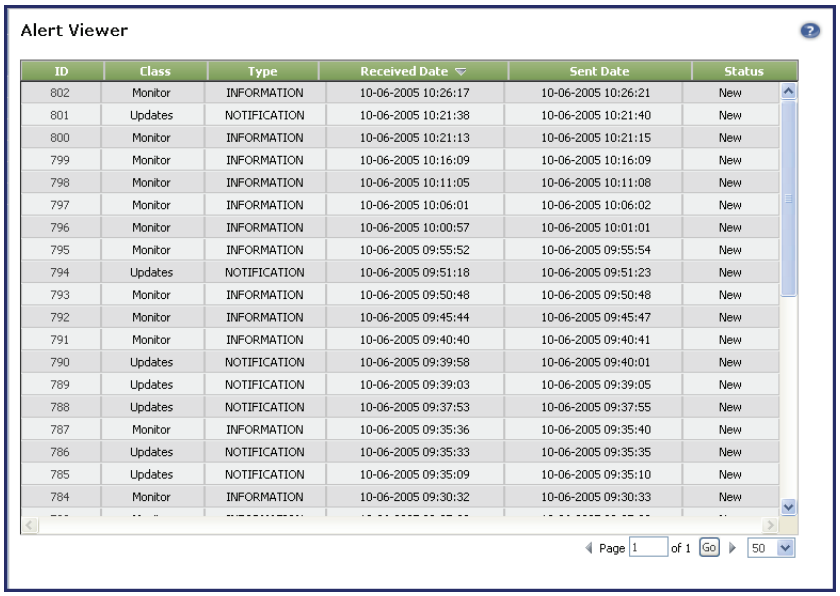


For this mechanism, you must supply the server name as before, plus the SNMP version to be used and the port over which the alert will be transmitted. When you click **Submit**, the screen will refresh.

The Alert Viewer

The Alert Viewer screen presents an on-screen view of all the alerts IronMail has generated during the past three hours.

Reporting > Alert Manager > Alert Viewer



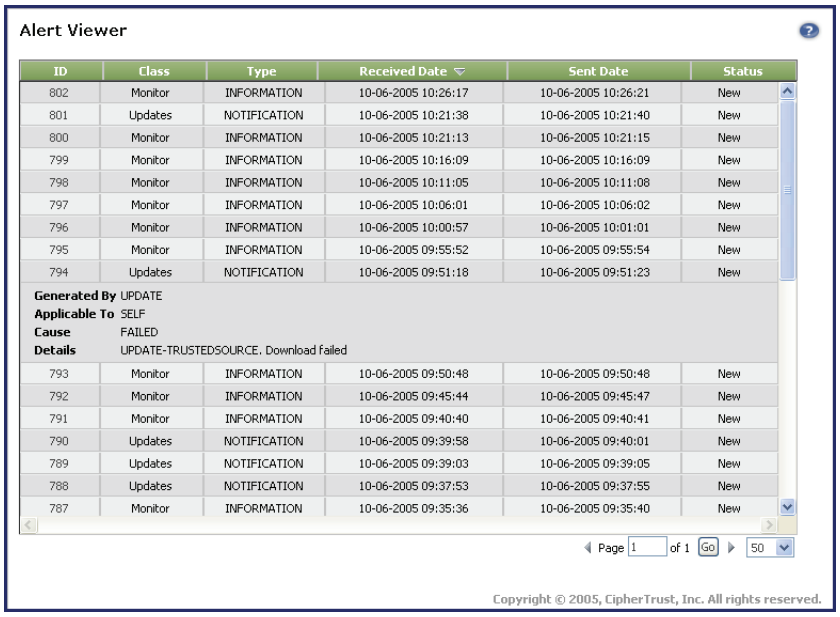
The Alert Viewer

Field	Description
ID	This column displays the internally-generated ID number of each alert. The ID number is also a hyperlink that opens a secondary browser window displaying details of the alert.
Class	This column displays the name of the class that contains the subsystem that generated the alert. The Class column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by class in ascending and descending order.
Type	This column identifies the level of the alert. The Type column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by alert level in ascending and descending order.

The Alert Viewer

Field	Description
Received Date	This column identifies the timestamp when the alert was generated. The Received Date column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by Received Date in ascending and descending order.
Sent Date	This column identifies the timestamp when the alert was delivered. The Sent Date column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by Sent Date in ascending and descending order.
Status	This column identifies the "status" of the alert, and will display one of two values: • **New:** This is a new alert for which delivery has not been attempted. • **Delivered:** IronMail successfully delivered the alert. • **Not Delivered:** IronMail has not yet delivered the alert. The Status column heading is also a hyperlink, allowing the administrator to sort the contents of the Alert Viewer table by Status in ascending and descending order.
Navigation	At the lower right of the screen you will find data fields and navigation arrows that will help you move through multiple pages of alerts.

When the alert ID hyperlink in the Alert Viewer table is clicked, the message line on the screen expands, displaying information about the alert. An example is included below.


Alert Viewer
ID
Class
Type
Received Date
Sent Date
Status
802 Monitor INFORMATION 10-06-2005 10:26:17 10-06-2005 10:26:21 New
801 Updates NOTIFICATION 10-06-2005 10:21:38 10-06-2005 10:21:40 New
800 Monitor INFORMATION 10-06-2005 10:21:13 10-06-2005 10:21:15 New
799 Monitor INFORMATION 10-06-2005 10:16:09 10-06-2005 10:16:09 New
798 Monitor INFORMATION 10-06-2005 10:11:05 10-06-2005 10:11:08 New
797 Monitor INFORMATION 10-06-2005 10:06:01 10-06-2005 10:06:02 New
796 Monitor INFORMATION 10-06-2005 10:00:57 10-06-2005 10:01:01 New
795 Monitor INFORMATION 10-06-2005 09:55:52 10-06-2005 09:55:54 New
794 Updates NOTIFICATION 10-06-2005 09:51:18 10-06-2005 09:51:23 New
Generated By UPDATE
Applicable To SELF
Cause FAILED
Details UPDATE-TRUSTEDSOURCE. Download failed
793 Monitor INFORMATION 10-06-2005 09:50:48 10-06-2005 09:50:48 New
792 Monitor INFORMATION 10-06-2005 09:45:44 10-06-2005 09:45:47 New
791 Monitor INFORMATION 10-06-2005 09:40:40 10-06-2005 09:40:41 New
790 Updates NOTIFICATION 10-06-2005 09:39:58 10-06-2005 09:40:01 New
789 Updates NOTIFICATION 10-06-2005 09:39:03 10-06-2005 09:39:05 New
788 Updates NOTIFICATION 10-06-2005 09:37:53 10-06-2005 09:37:55 New
787 Monitor INFORMATION 10-06-2005 09:35:36 10-06-2005 09:35:40 New
Page 1 of 1 Go 50
Copyright © 2005, CipherTrust, Inc. All rights reserved.

The Health Monitor

Health Monitor is an IronMail subsystem that examines the appliance's overall performance, running a series of tests to ensure that all services and processes are performing as designed. Health Monitor "wakes up" at a user-defined interval and runs automatically in the background to test its many subsystems. IronMail will also monitor the status of any internal servers that are "in-line" with IronMail (Health Monitor will send the mail server a connection request to ensure that it is responsive).

Note: If an intermediary device is between IronMail and the mail server, Health Monitor will incorrectly infer from the intermediary device's response that the internal server is functioning normally.

In this chapter

In this chapter you will find information about the following topics:

- Configuring Health Monitor
- Configuring Alerts

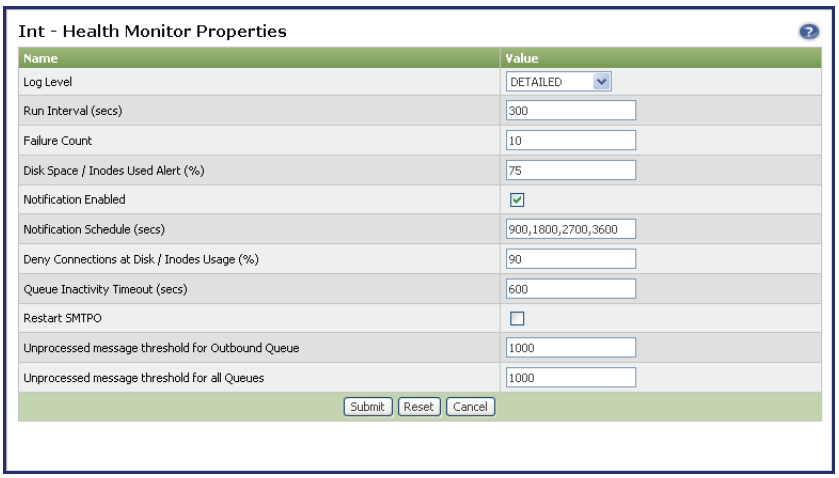
Configuring the Health Monitor

The Health Monitor screen provides access to the latest log detailing Health Monitor's activity. It also offers links that allow you to run a Health Monitor cycle on demand (**Run Now**), or access the properties screen where you may configure Health Monitor (**Configure**).

Administration > Health Monitor > Configuration

Health Monitor options may be configured by clicking the **Configure** hyperlink on the page. The Int-Health Monitor Service Properties window opens displaying Health Monitor's configuration options.

Administration > Health Monitor > Configuration > Configure



Health Monitor Properties

Field	Description
Log Level	IronMail offers 4 levels of logging, primarily to assist CipherTrust Support engineers when technical support is required. Select the log level you prefer. Options are: • Critical • Error • Information • Detailed
Run Interval (secs)	Enter a number representing, in seconds, the length of time from when the Health Monitor completes one run to when it starts another. It is recommended that this Run Interval not be set lower than the default 300 seconds (five minutes). During periods of high IronMail activity—e.g., heavy mail load—it may take several minutes or more for Health Monitor to finish its tests.

Health Monitor Properties

Field	Description
Failure Count	Enter a number representing how many times Health Monitor should repeat a failed system test before recording the failed test as an error. If this value is set to “10,” and a certain test fails 9 times but passes on the 10th try, IronMail does not record an error. Only if the test fails on the 10th successive attempt will IronMail log it as a error and move on to the next test. It is highly recommended that this default value (10) not be changed without first consulting with CipherTrust Technical Support. If “Notification” is enabled below, and IronMail’s Alert Manager is configured for it, IronMail will send an email, pager, or SNMP alert to the administrator when this occurs.
Disk Space/ Inodes Used Alert (%)	While there is a small disk partition devoted to the appliance’s operating system, all of IronMail’s program files, email Message Store, and temporary files reside on one, separate partition. The number entered in this input field represents how “full” the partition may become before generating an alarm. If “Notification” is enabled below, and IronMail’s Alert Manager is configured for it, IronMail will send an email, pager, or SNMP alert to the administrator when this threshold is reached. It is recommended that the default threshold (75%) be accepted in the beginning. After IronMail is fully “in-line” in the mail flow, and its logs and reports have accumulated on disk for several days, administrators can use IronMail’s System Graphs to view actual disk utilization. IronMail’s disk utilization may also be seen using the Command Line Interface.
Notification Enabled	If this option is enabled, Health Monitor will send alerts for any errors it detects to IronMail’s Alert Manager. Though the Alert Manager may receive the alerts from the Health Monitor, the alerts are not delivered to the administrator unless the Alert Manager has been configured to do so.

Health Monitor Properties

Field	Description
Notification Schedule (secs)	Health Monitor runs its tests on core subsystems and hardware every user-defined number of seconds (see "Run Interval" above). Rather than repeatedly generating alerts every time it detects the same error in successive tests, it will only generate alerts according to this "notification schedule." After the fourth notification, Health Monitor will continue sending alerts (if the condition persists) every nnn minutes, where nnn is the interval between the third and fourth notification. (E.g., if the notification schedule is 1 minute, 20 minutes, 1 hour, and 4 hours, subsequent notifications will be sent thereafter every three hours.) Enter four values, separated by commas, representing the number of seconds Health Monitor should wait before sending the same alert to IronMail's Alert Manager if, on a successive test, the condition still exists. Values must integers, and entered in increasing order.
Deny Connections at Disk/ Inodes Usage (%)	Enter a value, from 1 to 90, representing the maximum percentage of disk space utilization after which IronMail will stop accepting new messages. IronMail's SMTPI Service will stop accepting new SMTP connection requests when this threshold is reached. This value must be higher than the "Disk Space Used: Alert" value above.
Queue Inactivity Timeout	During Health Monitor's many tests, it looks at the time stamp when a message entered one of IronMail's queues, then compares it to the current system time. Taking into account how many messages are in the queue and IronMail's current "message load," if a message has remained in a queue more seconds than the number entered in this input field, Health Monitor will assume that particular Queue Service experienced a program error, and will stop and restart the service. If a "Queue Inactivity Time-out" is set to "0" (with the expectation that email should be processed by the queues *immediately*), Health Monitor may inaccurately report in its Detailed Log that a problem has occurred. That is, if there exists a slow pipeline to the internal mail server and/or high email volume, Health Monitor will report queue inactivity errors even though messages might be processed and flowing as expected. Initially, it is recommended that administrators accept the default period of inactivity of ten minutes (600 seconds). If the IronMail is processing large amounts of messages in a high email volume environment, the number of seconds may be increased.

Health Monitor Properties

Field	Description
Restart SMTPO	If, during its process, Health Monitor finds that SMTPO is not running, you have the option of restarting. If you want Health Monitor to restart SMTPO, select this checkbox.
Unprocessed Message Threshold for Outbound Queue	Enter a number of messages to serve as the threshold for the Outbound Queue. This integer represents the maximum number of unprocessed messages that should be in the queue. If the threshold is met or exceeded, Health Monitor will generate an Alert.
Unprocessed Message Threshold for All Queues	Enter a number of messages to serve as the threshold for all queues. This integer represents the maximum number of unprocessed messages that should be in any one of the other queues at any time. If the threshold is met or exceeded, Health Monitor generates an Alert.

When the information has been entered correctly, click **Submit** to save the configuration.

Clicking the View Log button opens the log file for Health Monitor. Detailed results of its tests appear in the log.

Health Monitor's Tests

Health Monitor Tests

Test	Test Name
httpd	Web Administration Test
sys-crypto	System Status Test - Crypto
sys-disk	System Status Test - Disk
sys-inode	System Status Test - Inode
sshd_maint	SSHD Command Line Interface (CLI) Test
tomcat	Web Administration JSP Test
sys-cmcsql	System Status Test - CMC IronMail SQL Connection Test
sys-cmcadmin	System Status Test - CMC IronMail Admin Connection Test
reports	Reports Test
admin	Admin Server Test

Health Monitor Tests

Test	Test Name
smtpo-count	SMTP Outbound Queue Count Test
smtpo	SMTP Outbound Queue Test
smtpproxy	SMTP Inbound Proxy Test
urq-tomcat	URQ Web Admin JSP Test

Configuring IronMail Alerts

You can configure the type of Alert that will be generated by each of Health Monitor's tests by clicking Configure Alerts. The following configuration screen opens.

Administration > Health Monitor > Configure Alerts

Configuring Health Monitor Alerts

Field	Description
Test Name	From the pick list, select the test for which you want to configure alerts. See Health Monitor Tests in the table above.
Error Alert Type	From the list, select the specific type of alert to be generated when Health Monitors detects an error from the specified test.
Success Alert Type	From the pick list, select the type of alert to be generated when the test runs successfully.
Restart Failure Alert Type	Select the specific type of alert to be generated when Health Monitor cannot restart the feature or function being tested.

When you have finished, click Submit to record your choices. If you want to generate alerts for every test, you must configure the alerts for each test individually.

Advanced Reporting

In this chapter

In this chapter you will find information about the following topics:

- Reports Configuration
- Detailed Logs
- Summary Logs

Reports Configuration

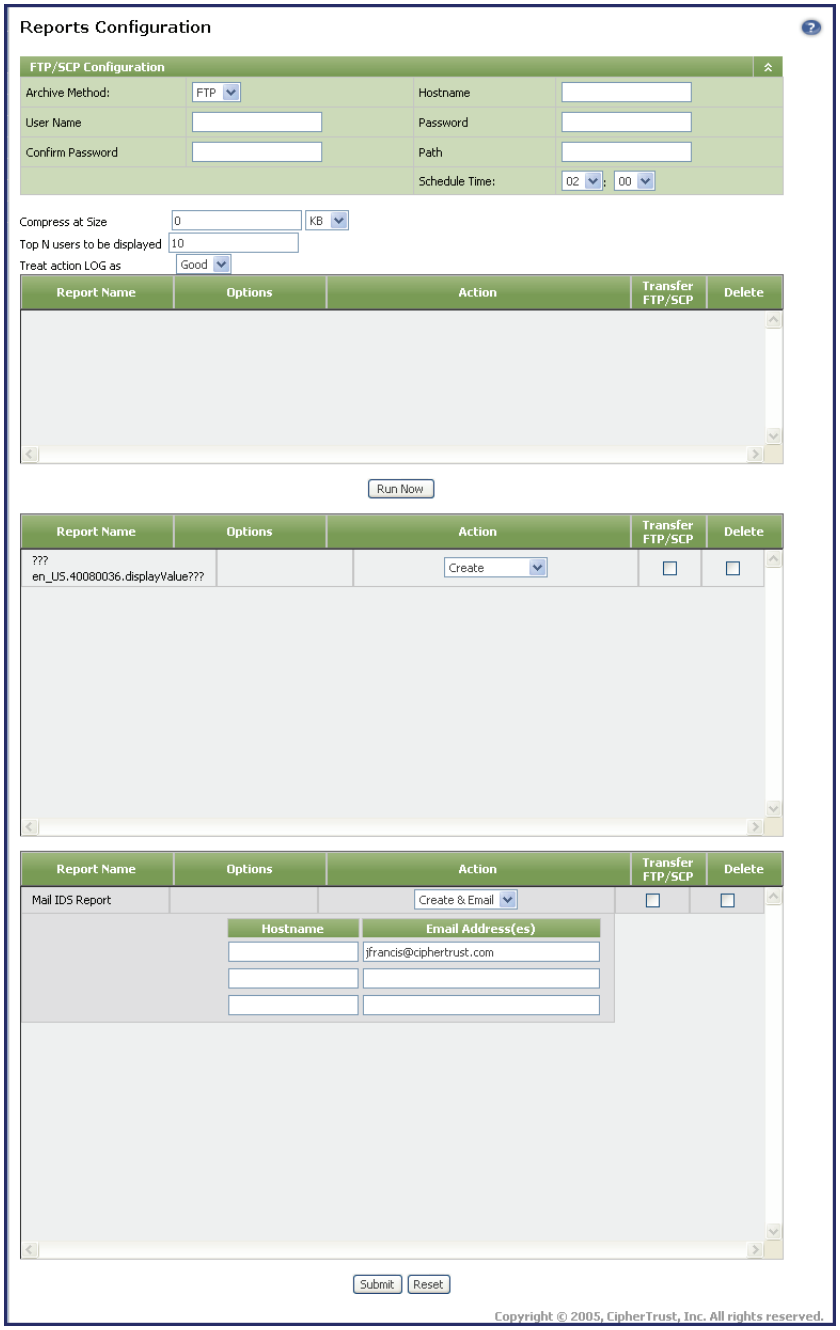
IronMail generates a variety of reports informing the Administrator of all of IronMail's activity. The reports cover two broad categories: the email that IronMail processes, and IronMail's internal activity.

Email activity can be viewed either as summaries or as detailed reports. The summaries show the top senders and receivers during a 24 hours period, who sent or received the most mail by volume (in megabytes), who sent or received the most encrypted messages, etc. Of particular interest to administrators is the summary report that provides spam statistics needed for decisions in a concise and easily understandable form.

All reports will be automatically sent to the recipient or recipients whose email addresses are specified if IronMail is configured to do so. In addition, IronMail will generate, "on demand," a report detailing every email policy that has been created. That is, you can view which Content Compliance "dictionaries" have been created and are in use, to whom Envelope Compliance policies have been applied, etc.

You can configure the reports that IronMail will generate and the disposition of the reports on the Reports Configuration screen.

Reporting > Advanced > Reports Configuration



Reports Configuration

Field	Description
FTP/SCP Configuration	*The top section of the screen is used to configure transfer and archiving for all reports.*

Reports Configuration

Field	Description
Archive Method	Select an archive method IronMail should use when transferring the Reports: • **SCP:** Select SCP to transfer the file securely using the SCP protocol. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the file in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files the hostname is appended to the file-name.
Hostname	Enter the host name of the archive server.
User Name	Enter a valid username with SCP or FTP privileges.
Password	Enter a valid password.
Confirm Pass-word	Confirm the password by entering it again.
Path	Enter the path string to the location on the archive server where IronMail should transfer the Reports. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally iden-tical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
Schedule Time	Select from the Hour and Minute pick lists a time when IronMail should automatically transfer the Reports. It is recommended that administrators choose a transfer time after 4 AM to allow enough time for the reports to run and rollover the previous days logs.
Compress at Size	Enter a number to represent, in MB, the size at which IronMail will compress reports to save disk space.
Top N users to be displayed	Enter a number to determine how many users will be displayed in each report (e.g., the top 10 or 15).
Treat action LOG as	When an action of LOG is triggered, how should the messages that triggered action be represented in the Executive Report: as “good” or “bad?”
The Reports List	*The lower portions of the screen are used to configure the individual reports.*

Reports Configuration

Field	Description
Report Name	This field in each block contains the name of the report being configured. See the list of report descriptions included below.
Options	Some reports have an associated Options list. It this list is present, select the option you prefer for this report. • Details - this option specifies that the report will show details of activity, but will not include the records that triggered activity. • Details and Records - this option configures the report to include both the details and the associated records.
Action	The Action pick list offers three options: • **Disable:** When disabled, the report is not generated. • **Create:** When selected, IronMail generates the report but does not automatically send it by email. The report may be viewed in the Web Administration interface, and may automatically and/or manually be transferred to an archive server via the SCP or FTP protocols. • **Create and Email:** When selected, IronMail generates the report and emails it to specified users. The report may also be viewed within the Web Administration interface, and may automatically and/or manually be transferred to an archive server via the SCP or FTP protocols.
Transfer FTP/ SCP	If the report is to be transferred (archived), select the check box.
Delete	Clicking the check box and subsequently clicking **Submit** will cause the report to be deleted.
Hostname	Enter the host name or the IP address of the server to which the reports are to be sent.
Email Address(es)	The **Email Address(es)** input field is disabled unless **Create and Email** was selected in the Action column. Multiple email addresses may be entered, with each address separated by a comma. (Do not enter spaces between commas and subsequent email addresses.)
Run Now	The four policy configuration reports shown in the top section of the reports list may be run on demand. These reports show the current configuration of the specified policies in IronMail.

When the information has been properly entered, click **Submit** to implement the configuration.

Report Descriptions

IronMail can produce the following reports, if configured to do so:

Report Descriptions

Report Name	Description
Executive Report	Summarizes total messages inbound and outbound, plus blocked messages inbound and outbound, for the day, week, month quarter and year. Useful in identifying trends.
Incoming Report	Provides totals and averages of inbound messages for one day, plus "Top Ten" statistics for key concepts.
Mail IDS Report	Shows the results of IronMail's intrusion monitoring and activity, password strength, denial of service protection, program and filesystem integrity, etc.
Outgoing Report	Provides totals and averages of outbound messages for one day, plus "Top Ten" statistics for key concepts.

Detailed Logs

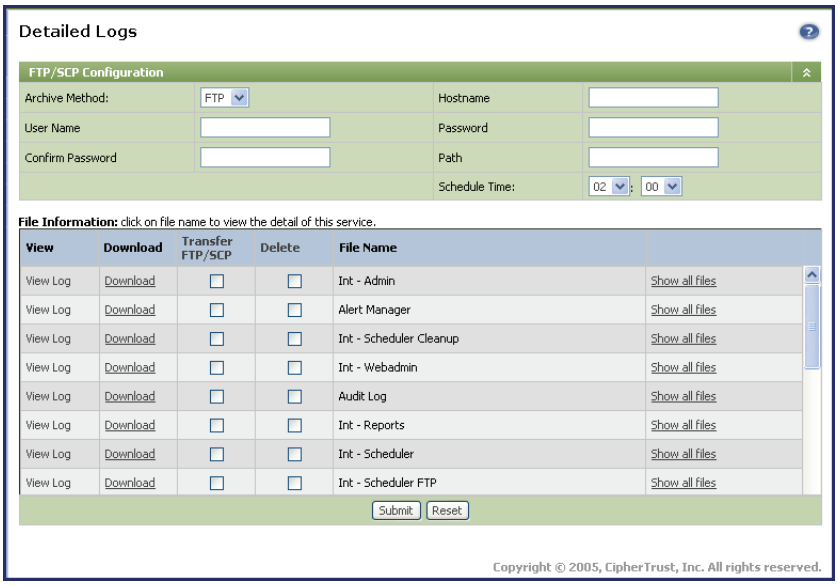
IronMail records in its Detailed Logs all the actions it takes as it processes messages. The amount of detail recorded in these logs is controlled by the Logging Level configured for each of IronMail's Queue Services and Mail Services. (For example navigate to Mail-Firewall > Configure Mail Services > SMTPI Service > "Log Level" in the secondary properties window for the SMTPI Service.)

Ordinarily, a log level of "Information" is adequate for day-to-day monitoring and will provide enough information to indicate that a Service is running properly, and at that level, will not bloat in size to an unmanageable level. It is recommended, however, that the logging level for Mail services (e.g., SMTPI/SMTPIS, POP3, POP3S, etc.) be set to "Detailed" for the first several weeks after IronMail is placed in the "mail flow" of the network. This will ensure that adequate information is available if troubleshooting mail-flow problems is required. Once IronMail is processing messages without incident, the logging level should be changed.

Similarly, the logging level for the Queue services (e.g., Content Filtering Queue, Anti-Spam Queue, etc.) should be raised to "Detailed" during the period that "policy testing" is underway. That level will be required to see the specific reasons a message was detected and acted upon by one of IronMail's spam or email policies. Once the *policy* testing is complete, these log levels may be changed.

In high mail-volume environments, some logs may grow very large, up to 100-200 MB in size. Log files larger than just 1 MB will typically take longer to open in IronMail's web interface than administrators will care to wait. Administrators are encouraged, then, to use an SSH client (such as the freely available "Putty" client) to open these logs. Within the command line interface, logs open instantly, and queries within them are as fast.

Reporting > Advanced > Detailed Logs



Detailed Logs

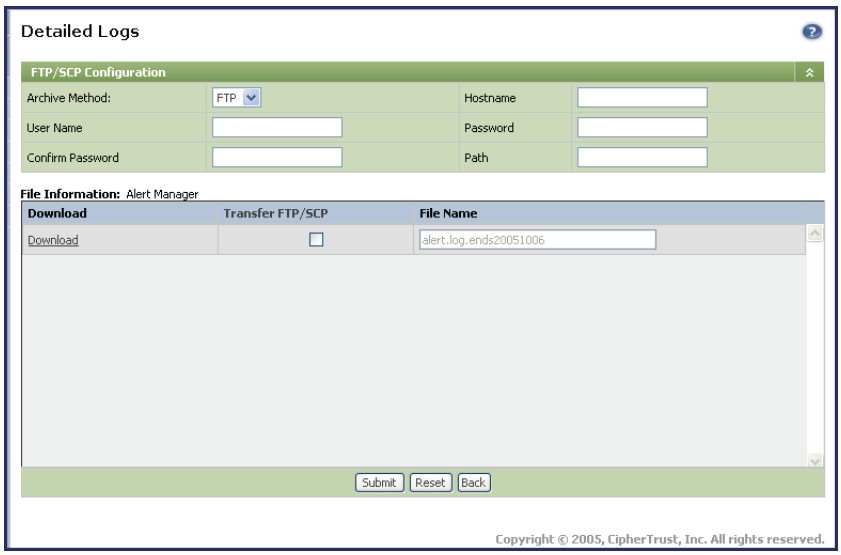
Field	Description
FTP/SCP Configuration	*The top portion of the screen is used to configure the archiving of the daily logs.*
Archive Method	Select an archive method IronMail should use when transferring the Logs: • **SCP:** Select SCP to transfer the file securely using the SCP protocol. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the file in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files the hostname is appended to the file-name.
Hostname	Enter the host name of the archive server.
User Name	Enter a valid username with SCP or FTP privileges.

Detailed Logs

Field	Description
Password	Enter a valid password.
Confirm Password	Confirm the password by entering it again.
Path	Enter the path string to the location on the archive server where IronMail should transfer the logs. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
Schedule Time	Select from the Hour and Minute pick lists a time when IronMail should automatically transfer the Logs. It is recommended that administrators choose a transfer time after 4 AM to allow enough time for the reports to run and rollover the previous days logs.
File Information	*The lower portion of the screen is a table that shows information about all the detailed logs.*
View	Click the hyperlink for any individual log file to open that file for viewing.
Download	Click the hyperlink for any log file to download that file.
Transfer FTP/ SCP	If the file is to be archived, click the check box.
Delete	Click the check box and then click **Submit** to delete the log.
File Name	This column lists by feature or function name the logs that IronMail generates.
Show all files	Clicking this hyperlink opens a screen that lists all available versions of the specific log. Log files remain available until they are deleted by the Cleanup process.

Clicking show all files opens a screen like the example shown below.

Reporting > Advanced > Detailed Logs > Show All Files



Detailed Logs - Show All Files

Field	Description
FTP/SCP Configuration	*The top portion of the screen is used to configure the archiving of the specific logs.*
Archive Method	Select an archive method IronMail should use when transferring the Logs: • **SCP:** Select SCP to transfer the file securely using the SCP protocol. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the file in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files the hostname is appended to the file-name.
Hostname	Enter the host name of the archive server.
User Name	Enter a valid username with SCP or FTP privileges.
Password	Enter a valid password.
Confirm Password	Confirm the password by entering it again.

Detailed Logs - Show All Files

Field	Description
Path	Enter the path string to the location on the archive server where IronMail should transfer the logs. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
File Information	The lower portion of the screen shows available logs of the type selected, in date order.
Download	Click the hyperlink for any log file to download that file.
Transfer FTP/ SCP	If the file is to be archived, click the check box.
File Name	This column lists the available versions of the specific log file in ascending date order.

A sample from a detailed log appears below.

```
ALERT:10062005 00:00:01:Starting Spin Run #39669
AlertSpinner:39669-10062005 00:00:01::No. of alerts in alertList: 0
AlertSpinner:39669-10062005 00:00:01::Ending Spinner thread.
ALERT:10062005 00:00:01:Ending   Spin Run #39669
ALERT:10062005 00:00:01:Sleeping       Run #39670
ALERT:10062005 00:00:06:No. of threads under work: 0
ALERT:10062005 00:00:06:Starting Spin Run #39670
AlertSpinner:39670-10062005 00:00:06::No. of alerts in alertList: 0
AlertSpinner:39670-10062005 00:00:06::Ending Spinner thread.
ALERT:10062005 00:00:06:Ending   Spin Run #39670
ALERT:10062005 00:00:06:Sleeping       Run #39671
ALERT:10062005 00:00:11:No. of threads under work: 0
ALERT:10062005 00:00:11:Starting Spin Run #39671
AlertSpinner:39671-10062005 00:00:11::No. of alerts in alertList: 0
AlertSpinner:39671-10062005 00:00:11::Ending Spinner thread.
ALERT:10062005 00:00:11:Ending   Spin Run #39671
ALERT:10062005 00:00:11:Sleeping       Run #39672
ALERT:10062005 00:00:16:No. of threads under work: 0
ALERT:10062005 00:00:16:Starting Spin Run #39672
AlertSpinner:39672-10062005 00:00:16::No. of alerts in alertList: 0
AlertSpinner:39672-10062005 00:00:16::Ending Spinner thread.
ALERT:10062005 00:00:16:Ending   Spin Run #39672
ALERT:10062005 00:00:16:Sleeping       Run #39673
ALERT:10062005 00:00:21:No. of threads under work: 0
ALERT:10062005 00:00:21:Starting Spin Run #39673
AlertSpinner:39673-10062005 00:00:21::No. of alerts in alertList: 0
AlertSpinner:39673-10062005 00:00:21::Ending Spinner thread.
ALERT:10062005 00:00:21:Ending   Spin Run #39673
ALERT:10062005 00:00:21:Sleeping       Run #39674
ALERT:10062005 00:00:26:No. of threads under work: 0
ALERT:10062005 00:00:26:Starting Spin Run #39674
AlertSpinner:39674-10062005 00:00:26::No. of alerts in alertList: 0
AlertSpinner:39674-10062005 00:00:26::Ending Spinner thread.
ALERT:10062005 00:00:26:Ending   Spin Run #39674
ALERT:10062005 00:00:26:Sleeping       Run #39675
ALERT:10062005 00:00:31:No. of threads under work: 0
ALERT:10062005 00:00:31:Starting Spin Run #39675
AlertSpinner:39675-10062005 00:00:31::No. of alerts in alertList: 0
AlertSpinner:39675-10062005 00:00:31::Ending Spinner thread.
ALERT:10062005 00:00:31:Ending   Spin Run #39675
ALERT:10062005 00:00:31:Sleeping       Run #39676
```

Summary Logs

Detailed Log files record the specific actions IronMail takes when processing messages, the information is spread across multiple files. The Summary Log consolidates all message processing data into one file, and displays the information in a slightly different way. If IronMail does not accept a message (e.g., the sending *IP address* is on IronMail's Local Deny List and the message is dropped by the SMTPI Service), the only line in the Summary Log for that message will look like the example above.

If IronMail accepted and processed the message, the first line of the Summary

Log for that message will look like the example at the left. For each message that IronMail processed, each IronMail Queue process will write a separate line indicating what action it took. To view all the lines in the Summary Log for a single message, use the "grep" command on the message ID.

The Summary Log displays seven pipe-separated ("|") fields of data. Each line in the Summary Log displays information about each IronMail process that examined or processed a message. Note that the descriptions of IronMail processes are not grouped together by message. The processes of multiple messages are commingled. As with the Detailed Logs, administrators must follow the "trail of bread crumbs" using the "Message Identifier" to trace a single message in this log. The Summary Log may be viewed in "real time" for troubleshooting and policy-tuning purposes, or it may be exported so that a third party application can perform advanced grouping, sorting, and querying within it.

The **first field** is the date and timestamp when the message was received by the SMTPI Service.

The **second field** is the "process ID"—a number used internally by IronMail to identify which IronMail processes are processing a message. For example, the JoinQ has one process number, while the SMTPO Service has another process number.

The **third field** is the "message identifier"—a number IronMail uses to uniquely identify a message. If the message is *accepted* by the SMTPI Service, the "message identifier" becomes the Message ID. See the first sample log entry above.

However, if the message is *not accepted* by IronMail (for example, the message is from an IP address that appears on a Deny List), this value will be the source IP address and port number. See the second sample log entry above.

The **fourth field** is the "Action" number—a "0" or "1"—indicating whether IronMail took an action on the message because of the rules of an email *policy*. A "0" means no action was taken—the message passed straight through IronMail untouched. A "1" means that IronMail performed some action on the message.

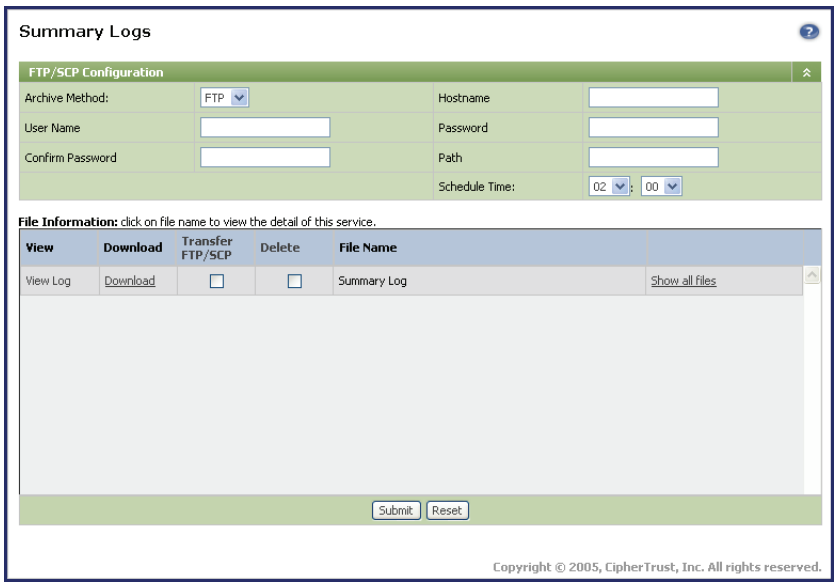
The **fifth field** is an internal numeric code representing the action IronMail took—a number representing, for example, whether IronMail stamped an outgoing message with a footer, or deleted a file attachment, etc. (See Action Codes for a list of all IronMail actions.)

The **sixth field** displays textual information returned by the process. For example, process "21" (the SMTPI Service) will return the Mail From, Mail To, and Message ID number of a message, and the "200" process (the Virus Scan Queue) will report "No virus found in this message."

The **seventh field** displays any details about the action as applicable. For example, a Mail Monitoring *rule* based on a particular Subject will have the text of the rule's Subject displayed here.

IronMail can transfer Summary Log files to an archive server, either manually or automatically.

Reporting > Advanced > Summary Logs



Summary Logs

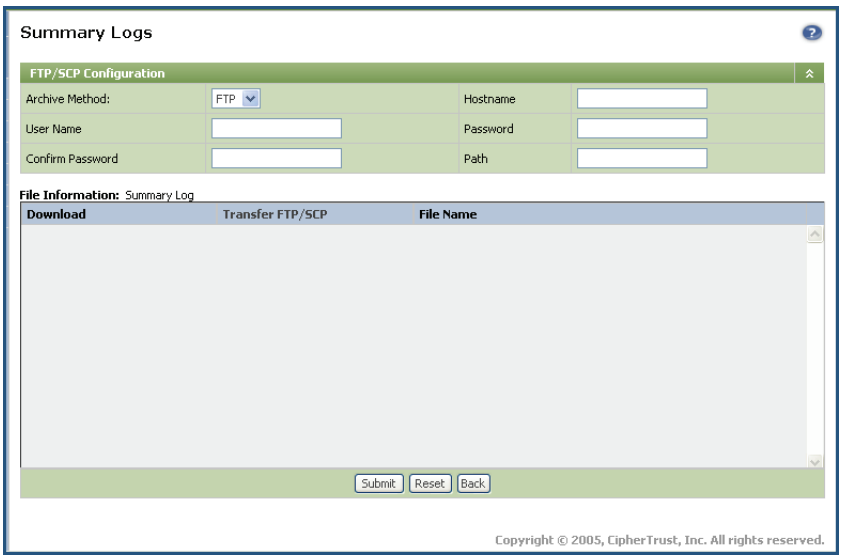
Field	Description
FTP/SCP Configuration	*The upper portion of the screen is used to configure archiving of the summary logs.*
Archive Method	Select an archive method IronMail should use when transferring the Logs: • **SCP:** Select SCP to transfer the file securely using the SCP protocol. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the file in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files the hostname is appended to the filename.
Hostname	Enter the host name of the archive server.
User Name	Enter a valid username with SCP or FTP privileges.
Password	Enter a valid password.

Summary Logs

Field	Description
Confirm Password	Confirm the password by entering it again.
Path	Enter the path string to the location on the archive server where IronMail should transfer the logs. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
Schedule Time	Select from the Hour and Minute pick lists a time when IronMail should automatically transfer the Logs. It is recommended that administrators choose a transfer time after 4 AM to allow enough time for the reports to run and rollover the previous days logs.
File Information	*The lower portion of the screen is a table that shows information about all the detailed logs.*
View	Click the hyperlink for any individual log file to open that file for viewing.
Download	Click the hyperlink for any log file to download that file.
Transfer FTP/ SCP	If the file is to be archived, click the check box.
Delete	Click the check box and then click **Submit** to delete the log.
File Name	This column lists the name of the log (Summary Log, in this case).
Show all files	Clicking this hyperlink opens a screen that lists all available versions of the specific log. Log files remain available until they are deleted by the Cleanup process.

Clicking the “show all files” hyperlink opens the list screen.

Reporting > Advanced > Summary Logs > Show All Files



Summary Logs - Show All Files

Field	Description
FTP/SCP Configuration	*The upper portion of the screen is used to configure archiving of the individual summary logs.*
Archive Method	Select an archive method IronMail should use when transferring the Logs: • **SCP:** Select SCP to transfer the file securely using the SCP protocol. (An SCP server must be configured and running on the archive machine.) • **FTP:** Select FTP to transfer the file in plain text (non-securely) using the FTP protocol. (The FTP server must be configured and running on the archive server.) Note that IronMail issues a *passive FTP* command. Note that if multiple IronMail appliances are configured to transfer files the hostname is appended to the file-name.
Hostname	Enter the host name of the archive server.
User Name	Enter a valid username with SCP or FTP privileges.
Password	Enter a valid password.
Confirm Password	Confirm the password by entering it again.

Summary Logs - Show All Files

Field	Description
Path	Enter the path string to the location on the archive server where IronMail should transfer the logs. Note: the "relative path" must be entered—that is the "starting point" or subsequent directory below which the user account has access privileges. Examples are: "/ironmail" or "./ironmail" (the two are functionally identical). Bear in mind that some Windows FTP servers may not translate on-the-fly forward slashes ("/") to back slashes ("\"). In those cases, back slashes are required as path delimiters.
File Information	The lower portion of the screen shows available logs of the type selected, in date order.
Download	Click the hyperlink for any log file to download that file.
Transfer FTP/ SCP	If the file is to be archived, click the check box.
File Name	This column lists the available versions of the specific log file in ascending date order.

X: Administration

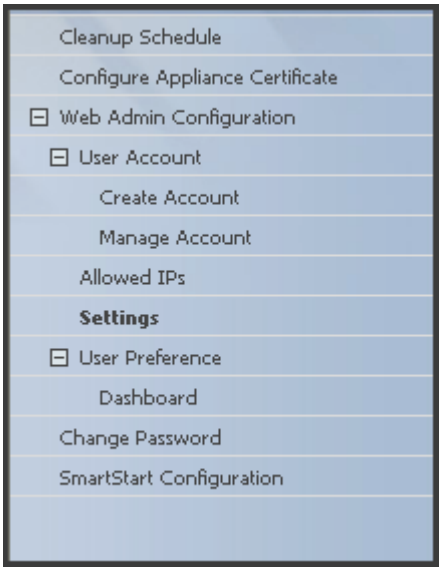
Introduction

The Administration program area provides the Administrator the means to manage user accounts on IronMail, to assist in maintaining the system, and to configure user preferences regarding the appearance and the behavior of specific screens and features.

In this section

In this section, you will find the following chapters:

- Chapter 10: Web Administration
- Chapter 11: General Administration



Configuring Web Administration

Web Administration is the functional area within Administration that includes allowing and controlling access to IronMail and the specific program areas within it. It also permits the Administrator to configure the specific appearance and content of certain screens.

In this chapter

In this chapter you will find information about the following topics:

- User Accounts
  - Creating Accounts
  - Managing Accounts
- Allowed IPs
- Settings
- User Preferences
  - Dashboard

User Accounts

The IronMail administrator may create user accounts for additional personnel who are granted permission to perform specific duties in administering the IronMail appliance. The administrator can select which program areas users are allowed to access, and whether their access is "read only" or "read/write."

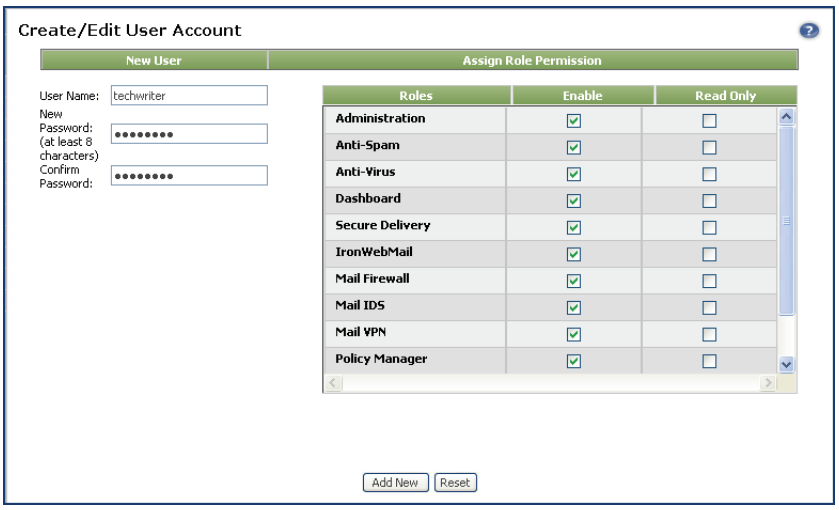
There is one "super user" account for the IronMail administrator. This "super user" account name is "admin." Only the admin user account has access to this User Accounts window. This allows the Administrator secure control over access to IronMail.

IronMail generates a daily log showing each user's login and the IronMail windows accessed.

Creating User Accounts

Only the Administrator (using the Admin super-user account) can create or edit user accounts. You can add or edit accounts using the Create/Edit User Account screen.

Administration > Web Admin Configuration > User Account > Create Account



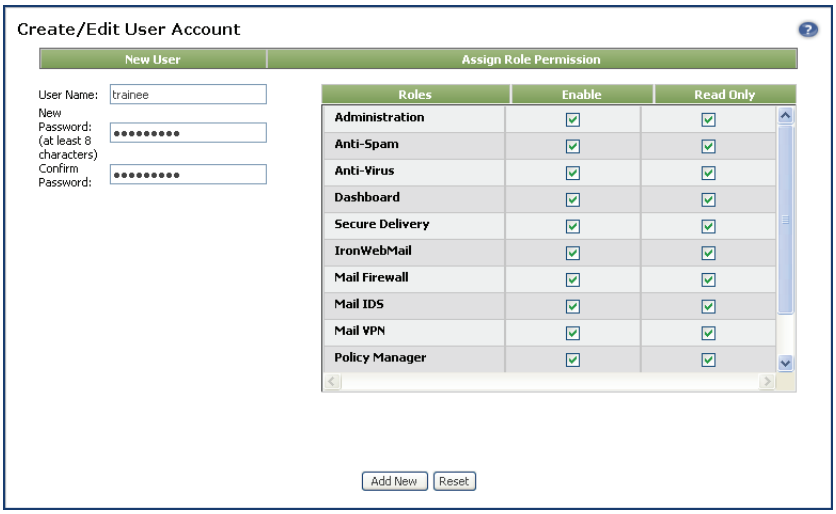
Adding or Editing User Accounts

Field	Description
New User	*The left side of the screen contains the data fields for naming the user and assigning a password.*
User Name	If you are adding a new account, enter the user name in this field. If you are editing an existing account, the name will already be populated. ***NOTE:*** The user name may be up to 16 characters long with no space. The following characters are allowed: • A-Z (first character only) • a-z, 0-9, _ (underscore) first character • a-z, 0-9, - (dash), _ (underscore) for second through 16th characters.
New Password	Enter the new password for the account. Passwords must be at least 8 characters long with no spaces. The following characters are allowed: • A-Z, a-z, 0-9, - (dash), _ (underscore) for all characters.
Confirm Password	Confirm the password by entering it again.
Assign Role Permission	*The right side of the screen contains a table that lets you grant or deny access to specific roles in IronMail and assign permissions for those roles where access is granted.*
Role	The first column shows all the available IronMail roles. The list is not configurable.

Adding or Editing User Accounts

Field	Description
Enable	Click the Enable checkbox to allow the user access to this role. If only the Enable box is checked for the role, the user will have full Read-Write permissions to that role.
Read Only	If a role is enabled, you can check this box to restrict permission to Read Only access.

For some users (such as new trainees) you may wish to assign Read-Only access to IronMail roles until the user has gained familiarity with IronMail and its features. Other users, by the nature of their positions, may require Read and Write access only to specific portions of the system. The Create/Edit User Account screen allows the Administrator to assign and change permissions as required.

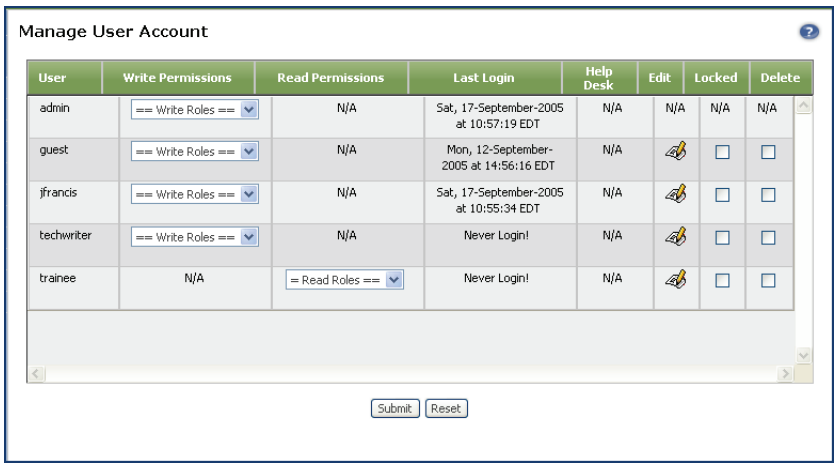


When the account is properly configured, click Submit. The new account will be added to the Manage User Account list.

Managing User Accounts

The Manage User Accounts link on the main IronMail page opens a screen that displays all existing user accounts for the specific appliance.

Administration > Web Admin Configuration > User Account > Manage Account



A table of user accounts is displayed. The table shows the logon name and program permissions for each user account. Until user accounts are created, only the "admin" super-user account is displayed.

Web Admin User Accounts

Field	Description
User	This column lists the user names for all users who have permissions on IronMail.
Write Permissions	If the user has write permissions for any roles, the pick list in this column will show all those roles. If no write permissions are granted, the column will display N/A.
Read Permissions	If the user has read-only permissions for any roles, the pick list in this column will show all those roles. If only write permissions are granted, the column will display N/A.
Last Login	This column displays the date and time of the user's last login. If the user has not yet logged in, the column will carry the message, "Never Login!"
Help Desk	If the user account has been designated a Help Desk account (via IronMail Secure Web Delivery), that fact will be indicated in this column. These accounts must go through a Help Desk function to change or restore their passwords, etc.
Edit	For all accounts other than the Admin account, an Edit icon appears in this column. Clicking the icon opens the Create/Edit User Account screen (see previous discussion) for that account, allowing the Administrator to make changes.

Web Admin User Accounts

Field	Description
Locked	If the account is locked for reasons such as exceeding the maximum number of unsuccessful login attempts, this box will be checked. The Administrator can unlock the account by clicking the box again (de-selecting it), or lock the account by checking it if circumstances warrant.
Delete	Clicking the check box and then clicking **Submit** will cause the account to be deleted from the user list.

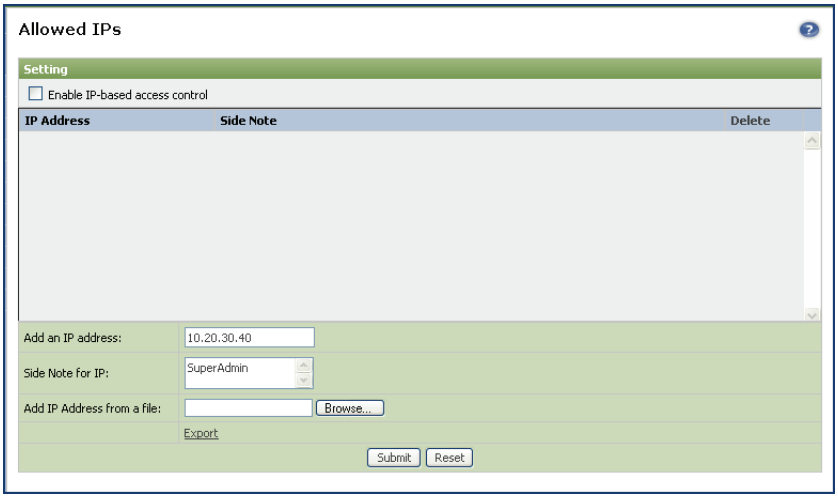
If you have made any changes to accounts on this list, click **Submit**. The changes will be implemented.

Allowed IPs

If the "Allowed IPs" option is enabled, IronMail will only accept browser connections (for Web Administration) from workstations or laptops with the IP addresses specified in the table on this page. If this option is not enabled, IronMail administrators may logon from any workstation.

WARNING: If "IP-based access control" (ACL) is enabled without entering valid IP addresses (i.e. addresses from which administrators may connect to IronMail), all IronMail administrators will be immediately locked out of the Web Administration interface. Administrators must logon to IronMail's Command Line Interface, either from an SSH client or via a keyboard and monitor attached to the appliance, and disable this setting. The CLI command to disable IP-based access control is: system restore acl (see the "System" commands in 'Command Line Interface' chapter of this User's Guide).

Administration > Web Admin Configuration > Allowed IPs



Allowed IPs

Field	Description
Enable IP-based access control	
Currently allowed IPs	The table near the top of the screen lists all the IP addresses that are currently allowed to access IronMail if IP-based access is enabled. Other user accounts will be blocked.
IP Address	This column displays IP addresses allowed to access IronMail's Web Administration interface.

Allowed IPs

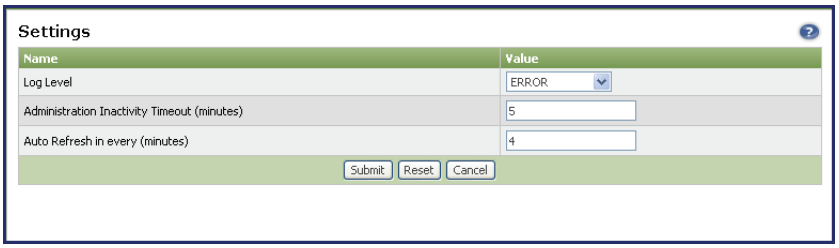
Field	Description
Side Note	This column displays any notes an administrator may have provided to "identify" to whom or where the IP address belongs.
Delete	Select an IP address' **Delete** check box and click **Submit** to delete an address from this table.
Adding new IP addresses	The data fields allow you to add new IP addresses to the permission list.
Add an IP Address	Enter an IP address. Subnets are not allowed.
Side Note for IP	Provide any text that may help identify or describe the IP address.
Add IP Address from a File	If a list of IP addresses already exists in a text file, they may be imported in one step, rather than being entered individually. The addresses must reside in a plain ASCII text file. Each address must appear on a separate line. **Browse** to the text file and click **Submit**.
Export	If you wish to store the current Allowed IPs list as a backup text file, click the Export hyperlink.

When the information is correctly entered, click **Submit** to implement the changes.

Web Admin Settings

The Settings screen allows the Administrator to configure specific behaviors for the Web Admin interface.

Administration > Web Admin Configuration > Settings



Web Administration Settings

Field	Description
Log Level	Select the log level from the drop down list. This setting determine the amount of detail entered into the logs regarding WebAdmin activity.
Administration Inactivity Timeout (minutes)	Enter a time in minutes at the expiration of which Web Admin will time out the user's login session due to inactivity, forcing a new login.
Auto Refresh in every (minutes)	Enter an interval in minutes to determine the refresh rate for Web Admin screens.

When the information is correctly entered, click **Submit** to implement the configuration.

User Preferences

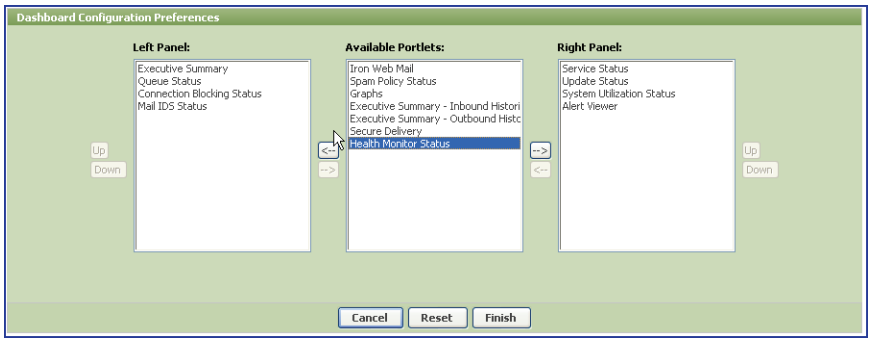
The Web Administration functions include configuration of the appearance of the Dashboard, based on user preferences.

Dashboard Preferences

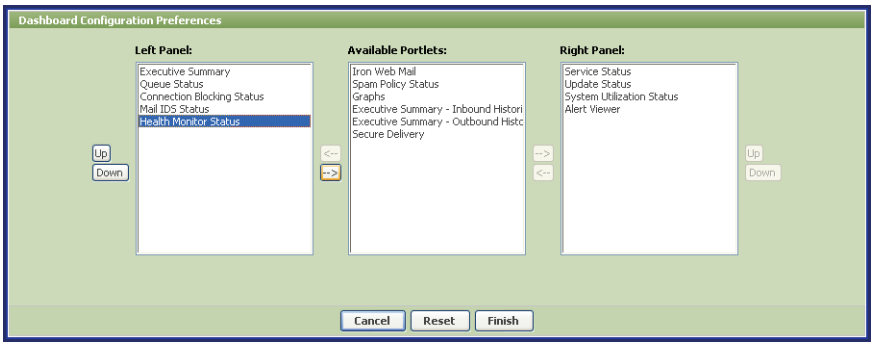
You can configure what reports, tables or graph appear on the Dashboard, and their location, using the screen below. The screen is also accessed from the Dashboard itself by clicking the "Configure" icon at the lower right corner of the Dashboard screen.

Administration > Web Admin Configuration > User Preference > Dashboard

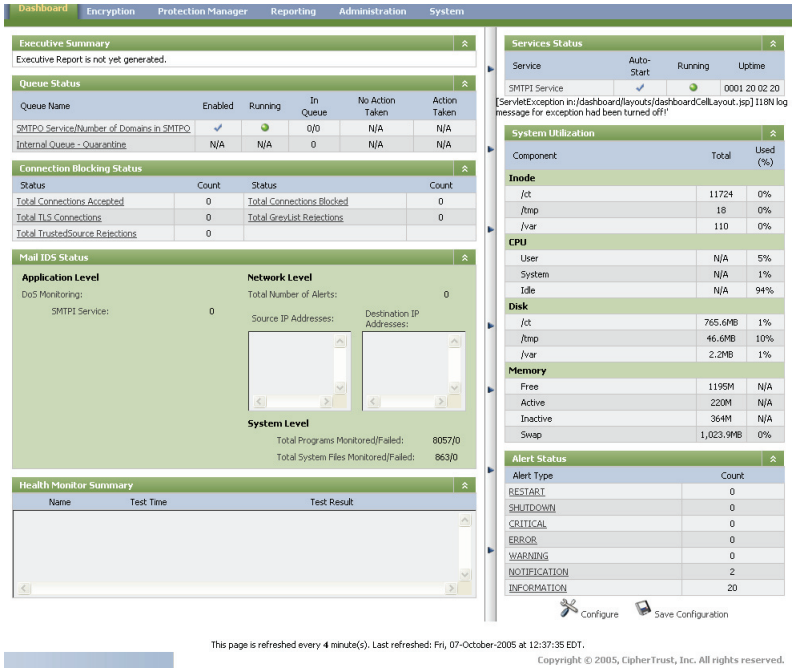
The center column of the Configure screen lists all portlets (each one representing a reporting mechanism) that have not been configured to appear on the existing Dashboard. To add a portlet to the Dashboard,, click the portlet to highlight it.



Then click the arrow pointing to the panel (**Left Panel** or **Right Panel**) where you want the new information to appear. The portlet will be moved to that panel, as shown below.



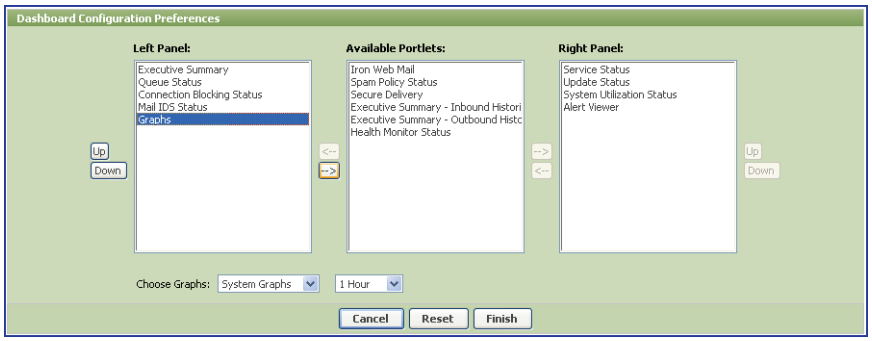
The new portlet is set to appear at the bottom of the panel, by default. If you want to change the placement of any portlet, highlight it and use the **Up** or **Down** button beside the panel. Click **Finish** to record the change.



The Dashboard is now updated to include the Health Monitor Summary.

If you want to remove a portlet from the Dashboard, go to the Configure screen, highlight the portlet, and click the arrow pointing to the **Available Portlets** panel. When you click **Finish**, the portlet will be removed from its display panel and added to the **Available Portlets** list.

One of the portlets that appear on the Configure screen is labeled **Graphs**. This selection allows you to move a series of graphs onto the Dashboard, and to determine which of three possible sets of graphs you want to display



Place the **Graphs** portlet in one of the display panels, just as you would any other portlet. When you click the arrow to move the portlet, the lower portion of the Configure screen displays two dropdown lists. The first list allows you to select which of the three types of graphs you want to display by default:

- System Graphs,
- Queue Graphs, or
- Executive Graphs.

The second list offers selections for the time period you want to represent with the selected graphs. The available periods vary with the type of graph you select, so choose the type first.

For more information about the reports and graphs on the Dashboard, go to Chapter 3 of this User's Guide.

General Administration Functions

In this chapter

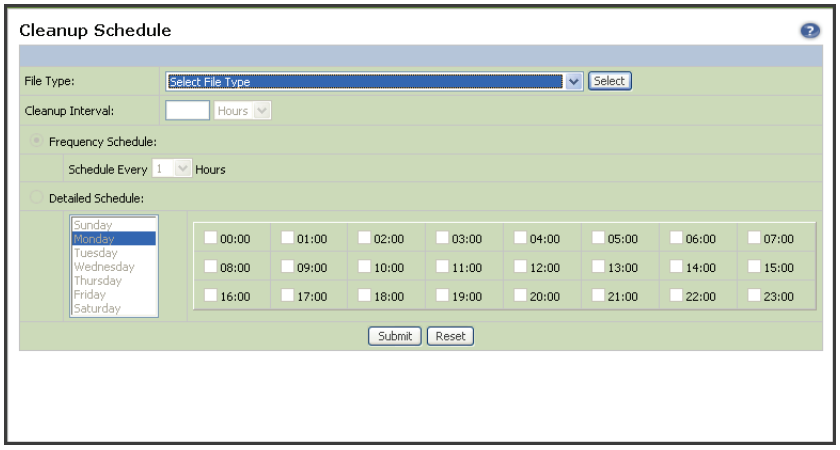
In this chapter you will find information about the following topics:

- The Cleanup Schedule
- Configuring Appliance Certificates
- Changing the Admin Password
- SmartStart Configuration

The Cleanup Schedule

IronMail accumulates many files and much data over time. CipherTrust recommends that you allow IronMail to regularly purge the system of unnecessary files and data. That is the function of the Cleanup Schedule.

Administration > Cleanup Schedule



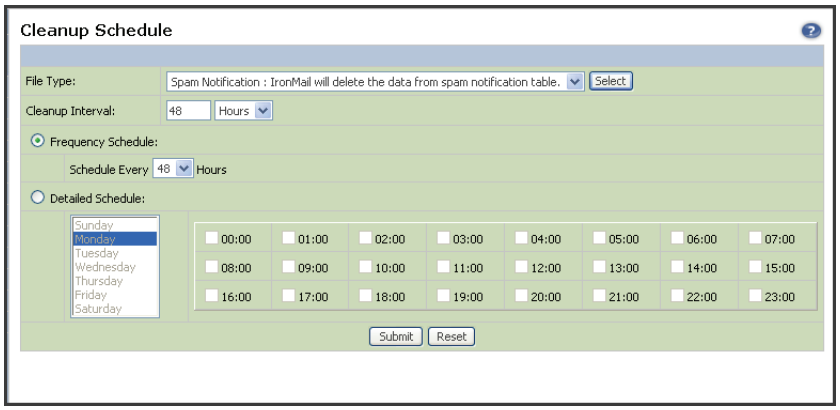
You must specify three options in order to configure the schedule:

- The files to be cleaned;
- The cleanup interval - how long a file may remain on the disk before it is cleaned from the disk; and,
- The cleanup cycle - how often (or when) the cleanup cycle will run.

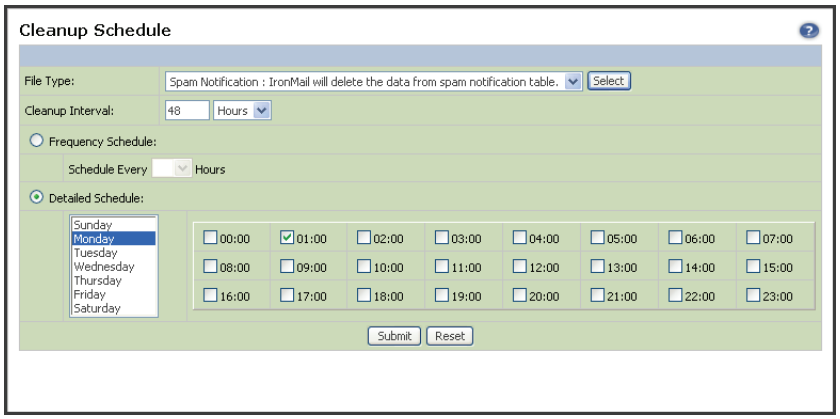
Cleanup Schedule

Field	Description
File Type	From the pick list, select the type of file for which you are configuring a cleanup schedule. Options are: • Database • Statistics • Log Files • Temporary Files • IDS Statistics • Quarantine Data • Spam Notification • SWD Viewed • SWD Non-Viewed Highlight the type and click the **Select** button.
Cleanup Interval	Specify the number of hours or days (by entering the number and selecting from the pick list) that this particular kind of file should remain in the database. IronMail converts “day” entries into hours internally.
Frequency Schedule	Clicking this button enables creation of a fixed-interval schedule for the Cleanup cycle. The Administrator may select an interval in hours (1 hour to 72 hours) between cycles. You must choose either Frequency Schedule or Detailed Schedule. Enabling one disables the other.
Detailed Schedule	This option allows creation of a specifically detailed schedule for the Cleanup cycle. The schedule is configured in two steps: • The left side of the screen displays a list of days of the week. Select the day during which the cleanup cycle is to run. You may select only one day at a time. However, after you submit the detailed schedule for one day, you can do it again for another day and the system will accumulate the daily schedules. It is therefore possible to create individual detailed schedules for all seven days per week. • The right side of the screen contains check boxes for each of the 24 hours in a day. Clicking a check box enables the CQS to run Auto Cleanup at that time on the designated day. You may select from 0 to 24 notification times per day.

To configure the schedule, first choose a file type. Click select to populate the screen with the current configuration, if one exists. If the file type has not been configured for cleanup, the screen is ready to accept the configuration. Select an interval and decide which cycle type you will use.



If you choose a Frequency Schedule, click the appropriate radio button and select a frequency (in hours).



If you prefer a Detailed Schedule, click that radio button. The select a day from the menu on the left side of the screen. On the right side, select the hours of the day when you want the Cleanup Cycle to run.

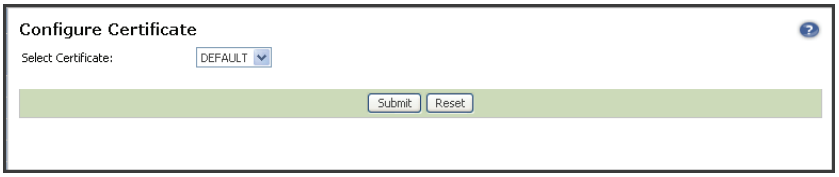
When you have completed setting the times for one day, you may pick another day and repeat the process. Continue until you have set up your complete weekly schedule.

When the configuration has been properly entered, click **Submit** to implement the new Cleanup Schedule.

Configuring Appliance Certificates

This screen is used to select the X.509 Certificate IronMail will use for SSL encryption. All installed X.509 certificates will show on the pick list. The Administrator selects one from the pick list and clicks **Submit**.

Administration > Configure Appliance Certificate

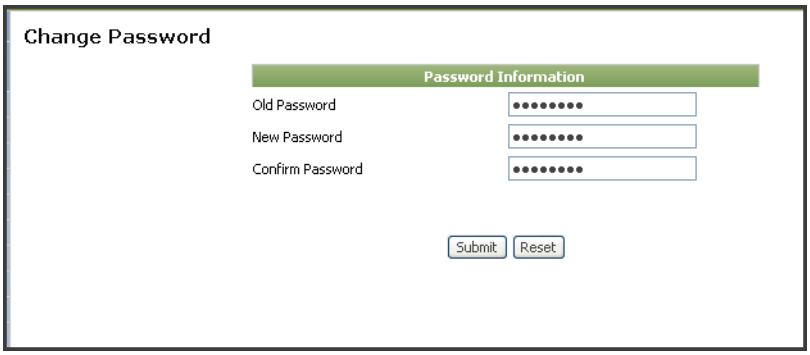


Although this function may be logically seen as part of Certificate Management, the screen is actually located under Administration.

Changing the Admin Password

Administrators are strongly encouraged to change the default Admin password (originally set as "password") during their first administrative session. After that, the password may be changed at any time, at the Administrator's discretion.

Administration > Change Password



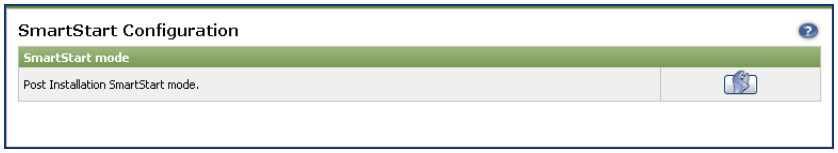
The Admin password may be changed, but the *admin* user name may not be changed or deleted.

SmartStart Configuration

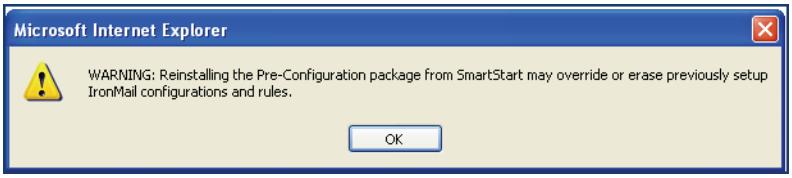
IronMail's SmartStart Configuration option first appears when a new IronMail appliance is deployed. After the Installation Wizard has been run to bring the appliance to a state where it can receive configuration options, SmartStart appears.

This same functionality is available to Administrators using the admin super-user account. This can be useful if SmartStart was not completed initially, and is no longer opening as the first screen after login.

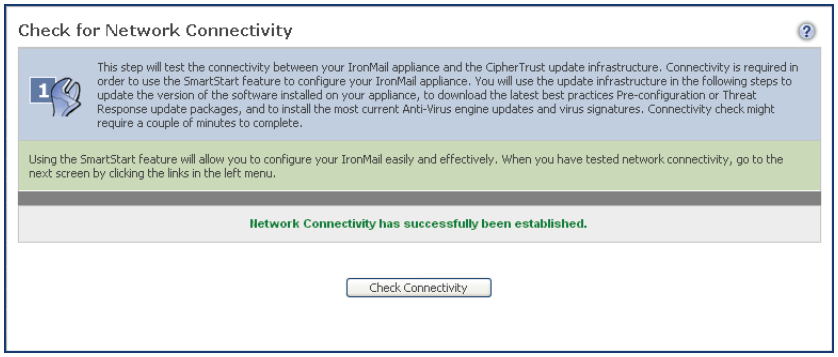
Administration > SmartStart Configuration



When the Administrator navigates to the SmartStart configuration option, the screen shown above displays. To continue with the option, click icon to the right. The following message box opens.


Microsoft Internet Explorer
WARNING: Reinstalling the Pre-Configuration package from SmartStart may override or erase previously setup IronMail configurations and rules.
OK

To continue with SmartStart, click OK. The opening screen for SmartStart appears.


Check for Network Connectivity
This step will test the connectivity between your IronMail appliance and the CipherTrust update infrastructure. Connectivity is required in order to use the SmartStart feature to configure your IronMail appliance. You will use the update infrastructure in the following steps to update the version of the software installed on your appliance, to download the latest best practices Pre-configuration or Threat Response update packages, and to install the most current Anti-Virus engine updates and virus signatures. Connectivity check might require a couple of minutes to complete.
Using the SmartStart feature will allow you to configure your IronMail easily and effectively. When you have tested network connectivity, go to the next screen by clicking the links in the left menu.
Network Connectivity has successfully been established.
Check Connectivity

For complete information about using the SmartStart Configuration Process, see Chapter 2 of this User's Guide.

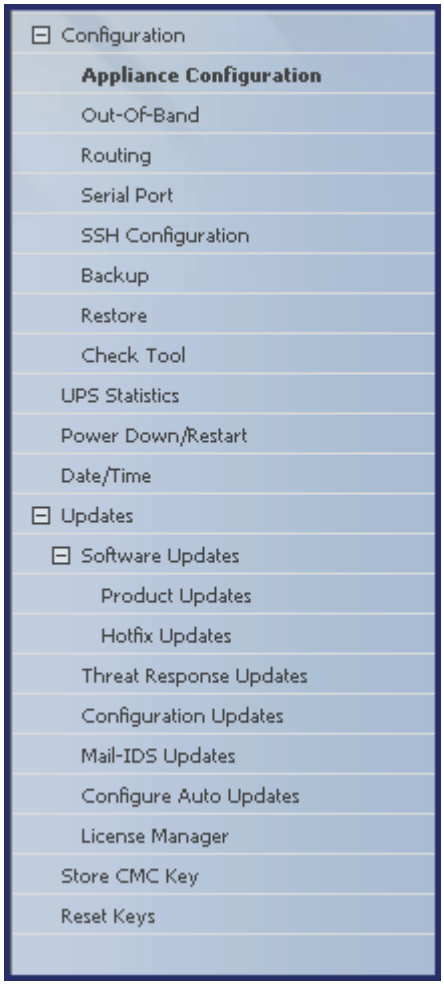
VII: System

The System program area in IronMail is particularly useful to Administrators who must configure system behavior as it will be encountered by the end users. This area allows configuration of the IronMail appliance itself with regard to basic parameters. It also permits the Administrator to make updates available to users, and to perform general system maintenance.

In this section

In this section, you will find the following chapters:

- Chapter 12: Configuration
- Chapter 13: Updates
- Chapter 14: Other System Functions



System Configuration

The Configuration program area is used to change settings related to the IronMail appliance itself.

In this chapter

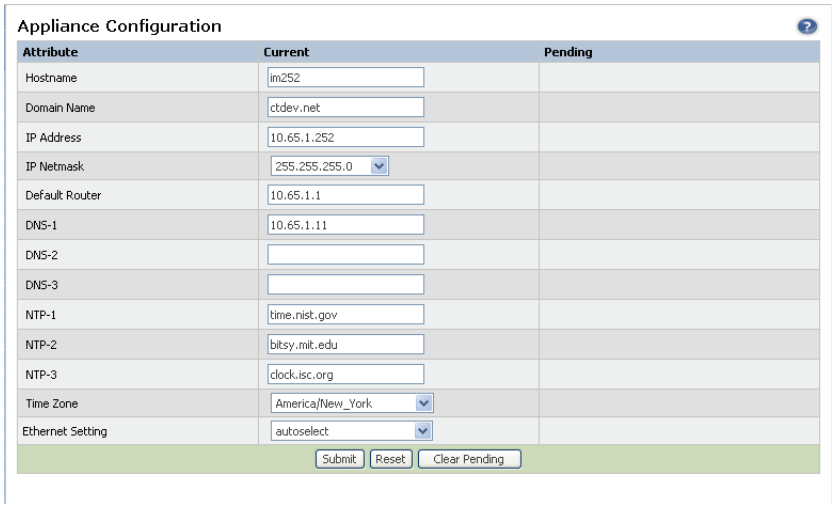
In this chapter you will find information about the following topics:

- Appliance Configuration
- Out-of-Band Management
- Routing
- The Serial Port
- SSH Configuration
- Backup
- Restore
- The Check Tool

Appliance Configuration

Initially, the Appliance Configuration screen displays information that was entered during the Initial Configuration Wizard when IronMail was first installed. At any time afterward, these settings may be changed as required.

System > Configuration > Appliance Configuration



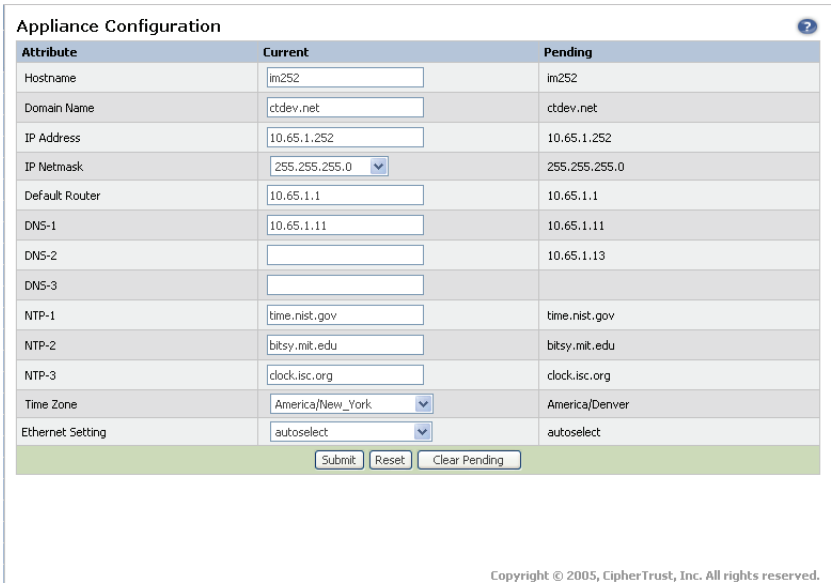
Appliance Configuration

Field	Description
Hostname	Enter a host name for the IronMail appliance. The host name must be entered in all lower-case letters for IronMail's Backup and Restore utilities to function correctly. This name must be resolved in DNS.
Domain Name	Enter the domain name to which IronMail belongs.
IP Address	Enter IronMail's IP address. (The host name and IP address must be resolved in DNS.)
IP Netmask	Enter the subnet mask required by the IP address.
Default Router	Enter the IP address of the default router.
DNS-1	Enter the IP address of the primary DNS server. (At least one DNS server must be provided.)
DNS-2	Enter the IP address of a secondary DNS server. (A second DNS server is optional.)
DNS-3	Enter the IP address of a tertiary DNS server. (A tertiary DNS server is optional.)
NTP-1	Enter the fully qualified domain name of a Network Time Protocol time server. IronMail will synchronize its internal system clock with this server. IronMail will query the NTP server once every minute. It the NTP server is unavailable, IronMail will query a secondary and tertiary NTP server if their names are provided immediately below.
NTP-2	Enter the fully qualified name of a secondary NTP server. IronMail uses this only as a backup if the first NTP server cannot be reached. IronMail does not "average" the time between multiple time servers.
NTP-3	Enter the fully qualified name of a tertiary NTP server. IronMail uses this only as a backup if the first and second NTP servers cannot be reached. IronMail does not "average" the time among multiple time servers.
Time Zone	Select from the **Time Zone** pick list a city that belongs to the same time zone where IronMail is located.

Appliance Configuration

Field	Description
Ethernet Setting	"Ethernet Settings" was not part of the Initial Configuration Wizard. Use this setting to resolve network difficulty that may be experienced when IronMail is physically connected to a network router or switch. While most hardware is designed to automatically negotiate an Ethernet "handshake," and agree on a speed and duplex mode, auto-negotiation is not always successful. Administrators must know the specific Ethernet settings of the hardware to which IronMail is physically connected. Select from IronMail's **Ethernet Settings** pick list a matching configuration. The Ethernet setting by default is "Autoselect." You may set it for the other available settings as required. However, should IronMail display erratic behavior with large files (>100kB), return the Ethernet Setting to "Autoselect."

To change the configuration of the appliance, make changes to any the fields on the screen. When the changes have been made, click **Submit**. The screen will refresh as shown below.



Now all the configuration parameters as they will appear if you continue with the changes are visible in the Pending column. This gives you a chance to do a final review before the changes are actually implemented.

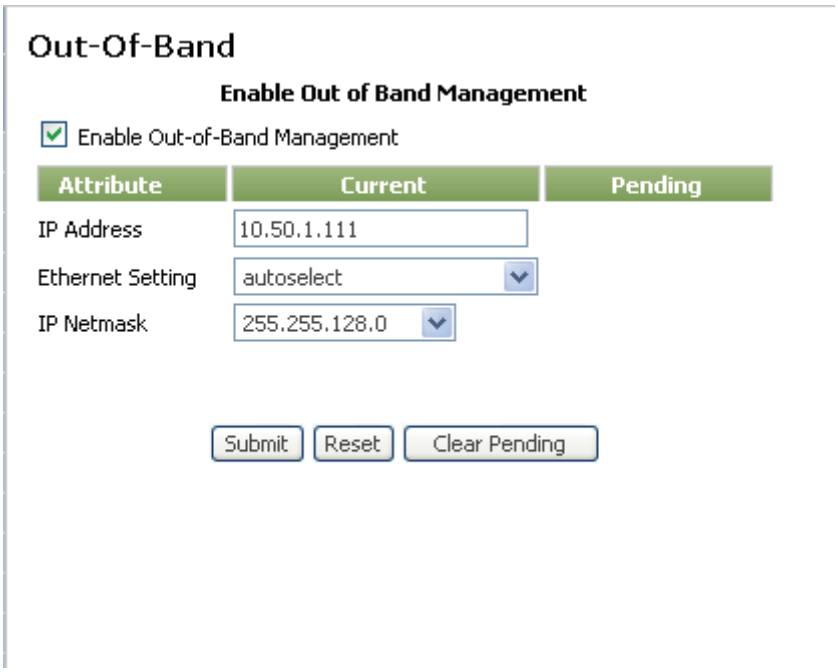
If you want to implement the changes, click **Submit** again. If not, click **Clear Pending**. The former configuration remains unchanged.

Out-of-Band Management

Only configurable and visible in IronMail appliances containing two network interface cards, this window allows administrators to use separate NICs and IP addresses for IronMail administration and mail processing. Email will flow through the first NIC, while Web Administration and Command Line management of the appliance occur on the second NIC. This allows management of the IronMail through a connection (out of band) that is not accessible to anyone using the normal email flow channels (in-band)

After the Initial Configuration Wizard reboots the IronMail appliance after the initial network settings are entered at the time of installation, the presence of a second NIC will be auto-detected and the administrator will be prompted to enter the network parameters of the additional card. To ensure maximum security, the second NIC should not be placed on the same network segment as the internal mail server. Use the input fields on this page to make subsequent changes to the second NICs network values.

System > Configuration > Out-of-Band



Out-of-Band Management

Field	Description
Enable Out-of-Band Management	Click the check box to enable management of the appliance via a secondary network interface card, rather than via the same interface that is used for mail flow.
Attribute	The names of the attributes that must be configured are listed in this column: • IP Address - Enter the IP address for the second network interface card. • Ethernet Setting - select the appropriate netmask from the drop-down list. • IP Netmask - Select the proper Ethernet setting from the list. You may choose to let the IronMail automatically select the appropriate setting, or choose from multiple options for 100baseTX or 10baseT.
Current	The current value or default for each attribute shows in the appropriate data field.
Pending	If you enter potential changes and click Submit, your new parameters will show in the Pending column. If you click Submit, they will be implemented. If you click Clear Pending, they will be deleted and the configuration will remain as it was.

After entering and/or selecting the required values, click **Submit**. The data will display in the Pending column to the right of the input fields. The data does not "take effect" until the appliance is rebooted.

Click **Clear Pending** to reset the input fields to their previous values.

Note: The IP address will be removed when Out-of-Band Management is disabled, in order to prevent it from remaining assigned, and therefore unavailable for reassignment.

Routing

When messages are addressed to mail servers that IronMail cannot directly reach (because IronMail is in a DMZ or for other reasons), a static route must be created so the mail IronMail proxies can be delivered to the internal mail servers. The Routing screen allows the Administrator to create this route.

System > Configuration > Routing

Routing

Field	Description
IP Address/Subnet	Enter the IP address of the machine that IronMail must deliver its mail to.
Netmask	Select from the **NetMask** pick list the subnet mask used by the machine.
Gateway	Enter the IP address of the gateway that knows how to reach the machine IronMail needs to deliver its mail to.
Delete	Select a machine's **Delete** check box and click **Submit** to delete a "route" from this table.
Adding new IPs or networks	*The data fields at the bottom of the screen permit the addition of new IP addresses or subnets.*
IP or Subnet	Enter a new IP address or subnet to be added to the table.
Netmask	Select the netmask from the drop down list.
Gateway	Enter the gateway IP address.

Adding a new IP address or subnet requires entering or selecting the necessary information. When the information is correctly entered, click **Submit**. The new entity will be added.

The Serial Port

IronMail's serial port may be configured for either one of two possible uses:

- as the connection port for an uninterruptable power supply, or
- as the access port for command line interface access using a keyboard (and monitor) connected directly to the IronMail appliance.

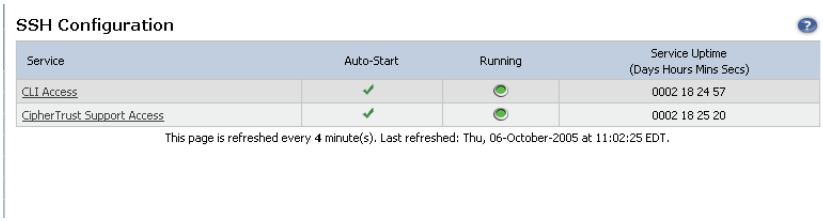
System > Configuration > Serial Port

To configure the serial port, the Administrator must select the desired use from the pick list, then click **Submit** to record the selection.

SSH Configuration

Accessibility to IronMail's command line interface is controlled by the "CLI Access Service." If this subsystem is not running, administrators will be unable to log onto IronMail via their favorite SSH client.

System > Configuration > SSH Configuration



SSH Configuration

Field	Description
Service	This column identifies the "CLI Access" Service. Two services are configurable: • CLI Access - allows the Administrator to use the command line to control the IronMail appliance. • CipherTrust Support Access - gives the Support Engineers remote access to the customer's IronMail to enable Support to assist, help solve problems, etc. The service names are hyperlinks allowing the Administrator to configure available details about each service.
Auto-Start	A red X or green check icon indicates whether or not the service is set to start automatically when the IronMail appliance is rebooted. If the icon is green, the service will begin running when IronMail restarts. In addition, if the icon is green IronMail's Health Monitor will restart a Service that has stopped for any reason when it performs its tests on all appliance subsystems. If an icon is red, the service will not start on reboot or when Health Monitor runs its system tests. (Note that a service can continue to run after its auto-start setting is turned off. A service cannot start running, however, until its auto-start setting is turned on.) The red and green icons are hyperlinks. Clicking the icon/hyperlink toggles the auto-start option on and off.

SSH Configuration

Field	Description
Running	A red or green light icon indicates whether or not the service is currently running. (Note that in some situations, the **Running** icon may not refresh when clicked, i.e. change from green to red, as expected. If the icon does not toggle, click the SSH Configuration hyperlink in the left navigation frame of the Web Administration interface to refresh the page, rather than clicking the **Running** icon a second time.)
Service Uptime	This column indicates (in days, hours, minutes, and seconds) how long a service has been running since it was last restarted.

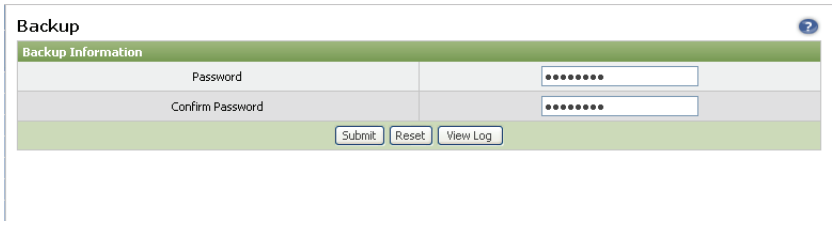
Clicking the CLI Access hyperlink on the SSH Configuration screen opens the CLI Access Properties screen. On this screen you can set the log level for Command Line Interface.

Similarly, clicking the CipherTrust Support Access hyperlink opens the associated properties screen. On this screen you can configure the port through which CipherTrust Support can access the appliance.

System Backup

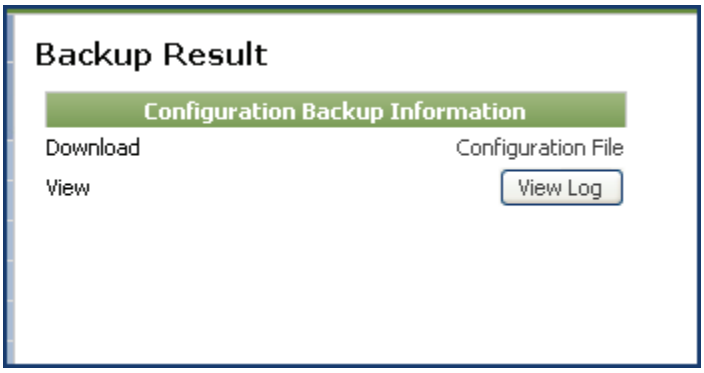
IronMail allows administrators to backup the configuration settings for the appliance (e.g., email policies, Mail and Queue Service settings, etc.) in case of disk failure. The backup should only be used to restore data to the same IronMail appliance.

System > Configuration > Backup



Enter and confirm a password to be associated with the backup file and click Submit. This password will be required when the backup is restored.

The following screen appears, confirming the action.



Click the **View Log** button to see the log describing the backup action.

```
BACKUP:09242005
15:35:53:**************************************************************************
* BACKUP:09242005 15:35:53:Args passed: DB:<> operation-
Type:<BACKUP> Push Components:<>
BACKUP:09242005 15:35:53:Backing up Database - ct
BACKUP:09242005 15:35:55:Backing up system files.
BACKUP:09242005 15:36:01:Custom pages backed up for system
backup
BACKUP:09242005 15:36:05:Encrypting using password.
BACKUP:09242005 15:36:06:Encoding the datafile -> /ct/w3/admin/java/
webapp/webadmin/tmp/im.6.0.0.20050924153553.zip
BACKUP:09242005 15:36:08:Cleaning the CMCTMP directory
BACKUP:09242005 15:36:08:Cleaning the CMCTMP directory done
BACKUP:09242005 15:36:08: Completed Operation Type : <BACKUP>
```

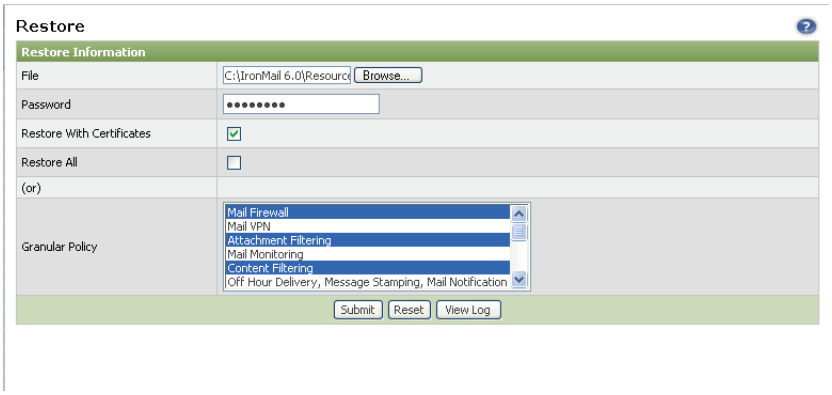
Clicking the Configuration File hyperlink will open a screen that provides information about the backup file and allows the Administrator to save the compressed folder for future use.

When IronMail saves a backup configuration to disk, it uses an automatic naming scheme, identifying the appliance's name, version number, latest release number, and date (e.g., im.4.5.1.1098287820.31.zip). The backup information is encrypted, stored in a proprietary file format that only IronMail can read, and cannot be viewed in Plain Text. The encryption method is "one way"—even CipherTrust Technical Support cannot decrypt this file. The "zip" file extension has been supplied to the backup file name solely for the purpose of "tricking" a browser into downloading the file, rather than trying to open it. Do not forget the password!

System Restore

Use the Restore function to restore data only to the same IronMail appliance. Software feature licenses—e.g., for IronWebMail, Secure Web Delivery, Anti-Virus, etc.—cannot be pushed to other appliances via this "restore" method.

System > Configuration > Restore



Restore

Field	Description
File	Enter the file name and its complete path, or browse to the backup file's location using the browse button.
Password	Enter the password associated with the backup file when it was created.
Restore with Certificates	Click the checkbox if you want to restore the security certificates that were in use by this IronMail when the backup was done.
Restore All	If you want to restore the complete database file, click the check box.
Granular Policy	If you prefer, you can click this check box and select the group or groups of policies to be restored.

Click **Submit** to execute the restoration. IronMail reads all the configuration data and enters it into the appliance. **The IronMail appliance will automatically reboot whenever a backup configuration is restored.**

Clicking the View Log button will open a log screen that provides details about the restoration.

When IronMail saves a backup configuration to disk, it uses an automatic naming scheme, identifying the appliance's name, version number, latest release number, and date (e.g., im.4.5.1.1098287820.31.zip).

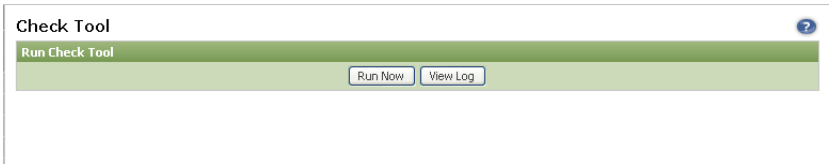
The name of the IronMail is stored within the backup file that is created. Therefore, under no circumstances rename or edit this file! Changing the file's name will cause the Restore function to fail, and may produce other unintended consequences.

Note: When an IronMail configuration is backed up, that appliance's host name, IP address/subnet, and User Accounts are saved. Restoring that backup configuration to another IronMail appliance will not overwrite the second box's host name, IP address, and subnet. However, the User Accounts will be restored—potentially creating a security risk. If the backup file from one IronMail is restored onto another IronMail, ensure that the User Accounts are carefully reviewed and modified as required.

The Check Tool

IronMail can test a variety of Network and Internet connections to ensure that the infrastructure supporting the internal email system is intact and fully functioning. Specifically, it ensures that connections to internal POP, IMAP, and SMTP servers can be opened, and that the DNS server is reporting the correct MX and A record data. Other network connections—such as network time, alerts, SLS sync, and LDAP servers—are also tested.

System > Configuration > Check Tool



Click **Run Now** to run the test. The screen will display a message acknowledging the job. When the job is finished, you can click **View Log File** to view a detailed log of the results of the test.

System Updates

Keeping IronMail current requires the Administrator to find and install the latest updates for a variety of services. The System program areal provides the necessary means for maintaining IronMail's effectiveness.

In this chapter

In this chapter you will find information about the following topics:

- Software Updates
  - Product Updates
  - Hotfix Updates
- TRU TrustedSource Updates
- Configuration Updates
  - Compliance Rules Updates
- Mail-IDS Updates
- Configuring Auto-Updates
- License Manager

Software Updates

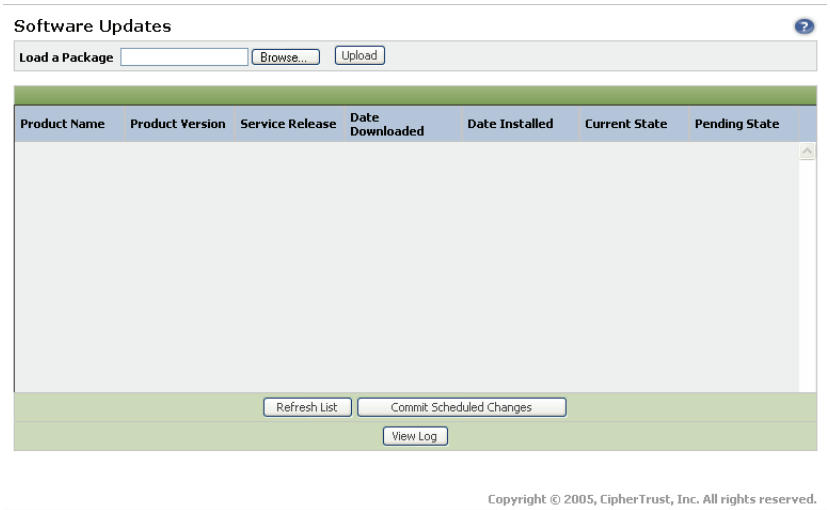
Two kinds of software updates are available:

- Product updates, which are new versions of the IronMail software or service releases containing new features and improvements; and
- Hotfix updates, which contain solutions to problems that have been discovered in existing releases.

Product Updates

The Software Updates table, empty until the CipherTrust Update Server has been queried, displays information about installed software and file updates available for installation.

System > Updates > Software Updates > Product Updates



Product Updates

Field	Description
Load a Package	If the update package you need resides in a file that may be downloaded, rather than on the update server, you can enter the complete path to the file or browse to it. When you click Submit, the package will appear on the update screen.
Available updates	*The table lists available software updates. To ensure the list is current, click **Refresh List** at the bottom of the screen..*
Product Name	This column displays the name of the CipherTrust product (e.g., IronMail or Centralized Management Console).
Product Version	This column displays the version number of the software. (The version of software this document describes is version 6.0.)
Service Release	This column displays the name of the Service Release. (Service Releases are named in incremental numbers in ascending order.)
Date Downloaded	This column displays the date when the software file was downloaded to IronMail's disk.
Date Installed	This column displays the date when the software file was installed on the appliance.

Product Updates

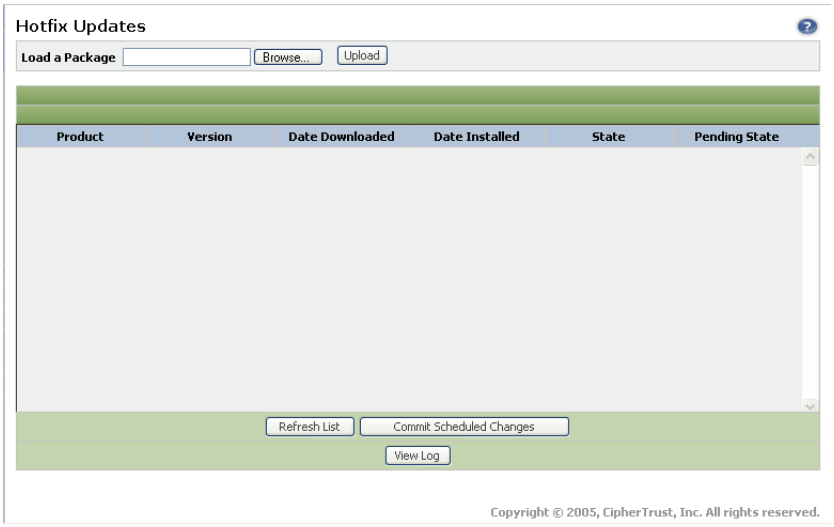
Field	Description
Current State	This column displays the software file current state. The "state" can be one of four values: • **Available:** The file is available and ready to be downloaded from CipherTrust's Update Server. • **Downloaded:** The file has been downloaded to disk, but has not yet been installed. It may be deleted or installed. • **Installed:** The file has been installed.
Pending State	If a file's status has changed (see immediately below), the new status is displayed in this Pending column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

The **Refresh List** button sends a request directly to CipherTrust's update server, which will populate your IronMail Software Updates page with its list of available file updates.

Hotfix Updates

Hotfix updates are shown on a separate screen.

System > Updates > Software Updates > Hotfix Updates



Hotfix Updates

Field	Description
Load a Package	If the update package you need resides in a file that may be downloaded, rather than on the update server, you can enter the complete path to the file or browse to it. When you click Submit, the package will appear on the update screen.
Available Hotfixes	*The table lists available Hotfixes. To ensure the list is current, click **Refresh List** at the bottom of the screen.*
Product	This column displays the name of the CipherTrust product (e.g., IronMail or Centralized Management Console).
Version	This column displays the version number of the software. (The version of software this document describes is version 6.0.)
Date Downloaded	This column displays the date when the software file was downloaded to IronMail's disk.
Date Installed	This column displays the date when the software file was installed on the appliance.
State	This column displays the software file current state. The "state" can be one of four values: • **Available:** The file is available and ready to be downloaded from CipherTrust's Update Server. • **Downloaded:** The file has been downloaded to disk, but has not yet been installed. It may be deleted or installed. • **Installed:** The file has been installed.
Pending State	If a file's status has changed (see immediately below), the new status is displayed in this Pending column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

As is true with software updates, the Refresh List button queries the CipherTrust Updates Server to ensure the latest available packages appear on the list.

Applying the Updates

The process for downloading and installing updates is identical for both types. Any value in each row of the table of software files is a hyperlink that opens a details screen. The details of the particular file are shown, and if the update is either Available or Downloaded, a Change State pick list allows the administrator to download or install the file. After clicking **Change State**, IronMail refreshes the previous

Software Update Management table, and the file's new status is displayed in the Pending Column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

Clicking the **View Log** File button opens a new browser window showing the status of the update process.

Threat Response Updates

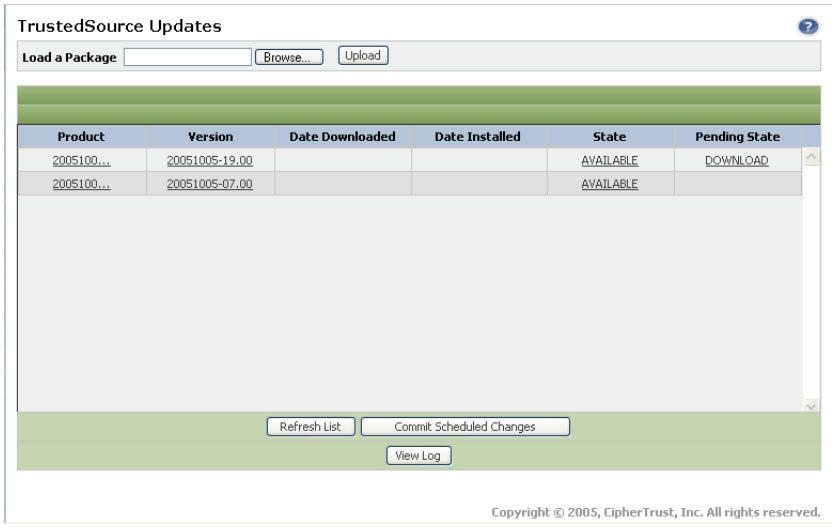
IronMail's Threat Response Updates make changes to specific configuration parameters within your system. These updates result from extensive research using the experiences and shared information from real customers. The intent is to keep your IronMail operating at peak effectiveness in light of current threats.

For IronMail Edge, TRU updates for TrustedSource are offered.

TrustedSource Updates

Navigate to the TrustedSource Updates screen to begin.

System > Updates > Threat Response Updates



TrustedSource Updates

Field	Description
Load a Package	If the update package you need resides in a file that may be downloaded, rather than on the update server, you can enter the complete path to the file or browse to it. When you click Submit, the package will appear on the update screen.
Available updates	*The table lists available updates. To ensure the list is current, click **Refresh List** at the bottom of the screen.*
Product	This column lists the product name for each update.
Version	The version number for the update displays in this column.

TrustedSource Updates

Field	Description
Date Down-loaded	This column displays the date when the software file was downloaded to IronMail's disk.
Date Installed	This column displays the date when the software file was installed on the appliance.
State	This column displays the software file current state. The "state" can be one of four values: • **Available:** The file is available and ready to be down-loaded from CipherTrust's Update Server. • **Downloaded:** The file has been downloaded to disk, but has not yet been installed. It may be deleted or installed. • **Installed:** The file has been installed.
Pending State	If a file's status has changed (see immediately below), the new status is displayed in this Pending column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

The **Refresh List** button sends a request directly to CipherTrust's update server, which will populate your updates page with its list of available file updates.

Any value in each row of the table of software files is a hyperlink that opens a "Change State" page in the main content page of the Web Administration interface. The details of the file are shown, and a Change State pick list allows the administrator to download or install the file. After clicking **Change State**, IronMail refreshes the previous Virus Updates table, and the file's new status is displayed in the Pending Column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

Configuration Updates

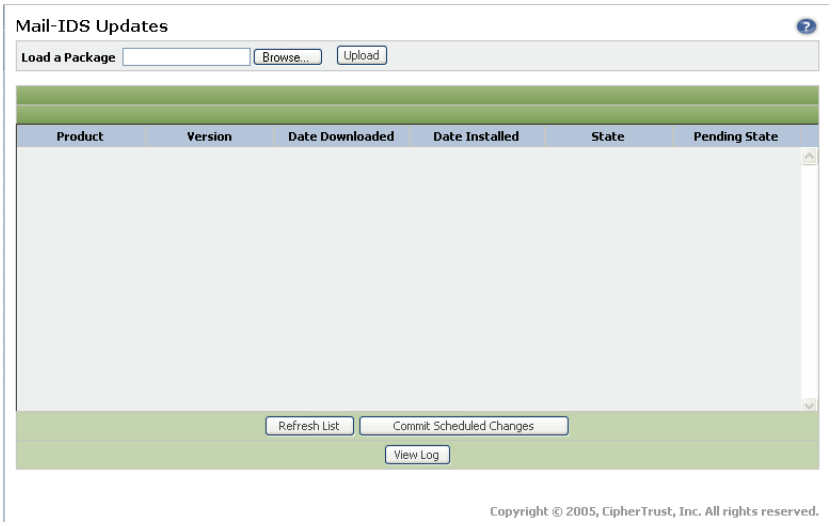
Proper protection for your email network requires keeping IronMail's configuration up to date. CipherTrust provides a variety of update packages to help Administrators maintain the latest, most effective configurations. Two of those update packages are available within the Compliance program area:

- Compliance Updates - intended to provide optimum configuration parameters for the Compliance functions; and,
- Pre-configuration Updates - providing the most effective initial configuration for newly deployed appliances.

Mail-IDS Updates

The Mail-IDS Updates table, empty until the CipherTrust Update Server has been queried, displays information about installed software and file updates available for installation.

System > Updates > Mail-IDS Updates



Mail-IDS Updates

Field	Description
Load a Package	If the update package you need resides in a file that may be downloaded, rather than on the update server, you can enter the complete path to the file or browse to it. When you click Submit, the package will appear on the update screen.
Available updates	*The table lists available updates. To ensure the list is current, click **Refresh List** at the bottom of the screen.*
Product	This column lists the product name for each update.
Version	The version number for the update displays in this column.
Date Downloaded	This column displays the date when the software file was downloaded to IronMail's disk.
Date Installed	This column displays the date when the software file was installed on the appliance.

Mail-IDS Updates

Field	Description
State	This column displays the software file current state. The "state" can be one of four values: • **Available:** The file is available and ready to be downloaded from CipherTrust's Update Server. • **Downloaded:** The file has been downloaded to disk, but has not yet been installed. It may be deleted or installed. • **Installed:** The file has been installed.
Pending State	If a file's status has changed (see immediately below), the new status is displayed in this Pending column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

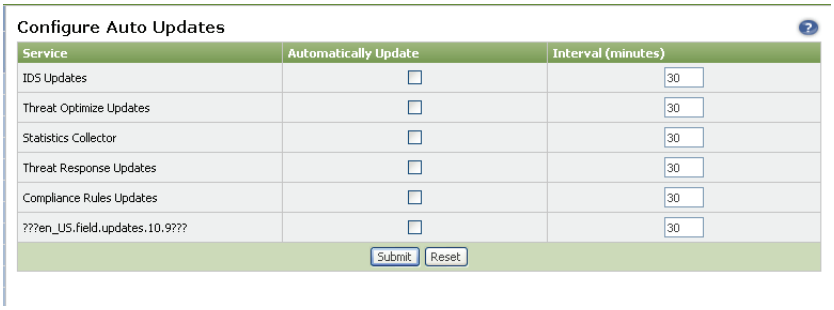
The **Refresh List** button sends a request directly to CipherTrust's update server, which will populate your updates page with its list of available file updates.

Any value in each row of the table of software files is a hyperlink that opens a "Change State" page in the main content page of the Web Administration interface. The details of the file are shown, and a Change State pick list allows the administrator to download or install the file. After clicking **Change State**, IronMail refreshes the previous Virus Updates table, and the file's new status is displayed in the Pending Column. The new status does not take effect until **Commit Scheduled Changes** is clicked.

Configuring Auto-Updates

The Configure Auto Updates sub-menu displays the licensed Subscription Services installed on the appliance. Each Service may be configured to query CipherTrust's update server for newly available files. IronMail will automatically download and install any files that become available.

System > Updates > Configure Auto Updates



Configuring Auto Updates

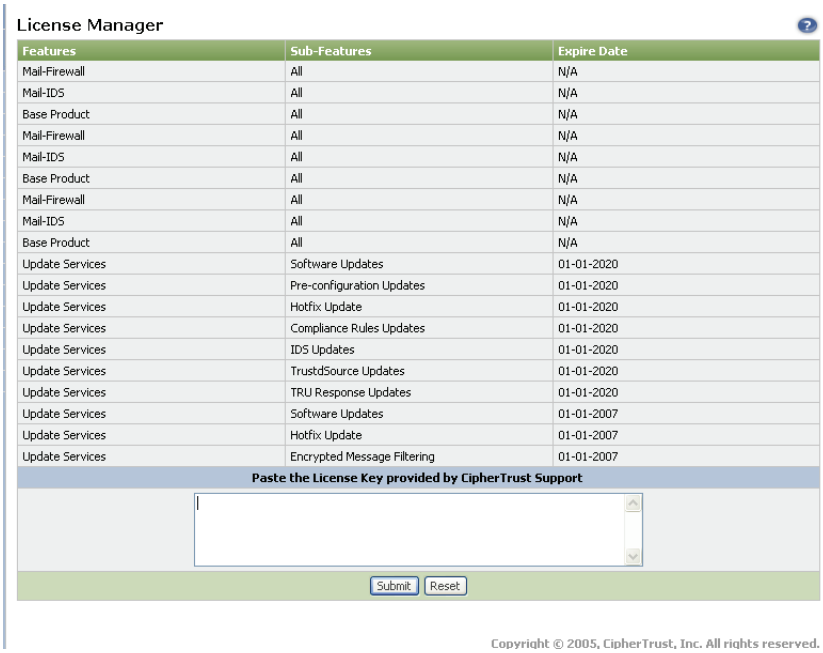
Field	Description
Service	The list of updatable services displays in this column.
Automatically Update	For each service you want to configure for automatic updates, click the checkbox in this column.
Interval (minutes)	For each updated service, specify the interval in minutes at which you want to query the update server for new updates. The default is 30 minutes.

When the services are configured appropriately, click **Submit** to record the configuration.

License Manager

The License Manager table shows all Product Licenses that have been installed on IronMail. Some of the Licenses correspond to the "tabbed" program areas in the IronMail interface (e.g., Mail-Firewall, Mail-VPN, etc.), where others refer to subscription services (e.g., Anti-Virus, Threat Response Updates, etc.).

System > Updates > License Manager


License Manager
Features
Sub-Features
Expire Date
Mail-Firewall All N/A
Mail-IDS All N/A
Base Product All N/A
Mail-Firewall All N/A
Mail-IDS All N/A
Base Product All N/A
Mail-Firewall All N/A
Mail-IDS All N/A
Base Product All N/A
Update Services Software Updates 01-01-2020
Update Services Pre-configuration Updates 01-01-2020
Update Services Hotfix Update 01-01-2020
Update Services Compliance Rules Updates 01-01-2020
Update Services IDS Updates 01-01-2020
Update Services TrustdSource Updates 01-01-2020
Update Services TRU Response Updates 01-01-2020
Update Services Software Updates 01-01-2007
Update Services Hotfix Update 01-01-2007
Update Services Encrypted Message Filtering 01-01-2007
Paste the License Key provided by CipherTrust Support
Submit
Reset
Copyright © 2005, CipherTrust, Inc. All rights reserved.

License Manager

Field	Description
Features	The licensable features installed on your IronMail are listed in this column.
Sub-Features	Each feature will have one or more subfeatures listed in this column. Some subfeatures are licensed separately.
Expire Date	The expiration date for each license is listed next to the associated subfeature. If license expiration does not apply, the column will show "N/A."
Paste the License Key provided by CipherTrust Support	For any license renewal, you will receive a new license key from CipherTrust Support. You must copy and paste that key into the available space. When you have done so, click **Submit** to renew the license.

Administrators can add licenses or extend the expiration date for product features or services at any time. (Licenses accumulate—that is, concatenate—on the appliance.)

Note: If a Secure Delivery license is installed after IronMail's initial installation, the administrator must logout and log back in to IronMail's Web Administration in order for the Secure Delivery program tab to display in the top navigation bar of the Web Admin interface. Also, when an anti-virus licenses expires, it disappears from the Web Administration interface and its functionality ceases on the midnight before the date of expiration. Anti-virus license renewals should be installed prior to license expiration. If a renewal license is installed after license expiration, administrators will have to manually re-configure anti-virus settings and place the Virus Scan Queue back into the Queue Order.

In enterprise environments where Centralized Management Consoles (CMC) are managing multiple IronMail "slaves," the CMC is responsible for acquiring and renewing all licenses. The CMC will automatically push product feature or service licenses to its IronMails.

While administrators were prompted to install a License Key when first running the IronMail Initial Configuration Wizard, they may install additional Licenses within this License Manager window. Paste in the License Number input field the "key" that CipherTrust Technical Support issued and click **Submit**. That program area that key enables is immediately available after logging out of the Web Administration interface and logging back in.

General System Functions

In this chapter

In this chapter you will find information about the following topics:

- UPS Statistics
- Powering Down and Restarting
- Setting Date and Time
- Storing CMC Keys
- Resetting Keys

UPS Statistics

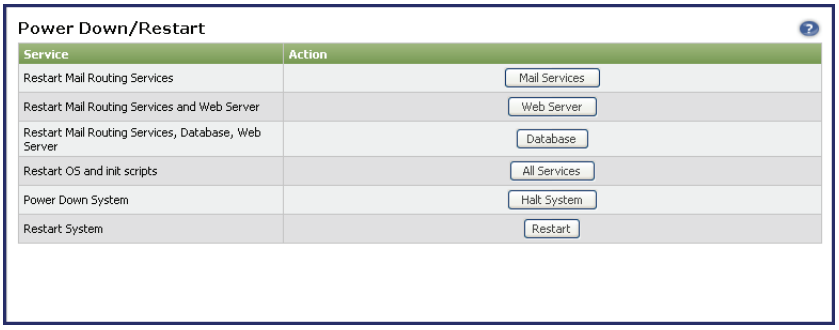
If IronMail is connected to a supported Uninterruptable Power Supply (UPS), it will display useful information about the status of the UPS. If IronMail is not connected to a supported UPS, this page will say that a UPS is not present.

System > UPS Statistics

Powering Down and Restarting

On occasion, it may be necessary to shut down the IronMail appliance or some portion of its processes. The Power Down/Restart screen allows you to do this gracefully with minimal risk of damage to files.

System > Power Down/Restart



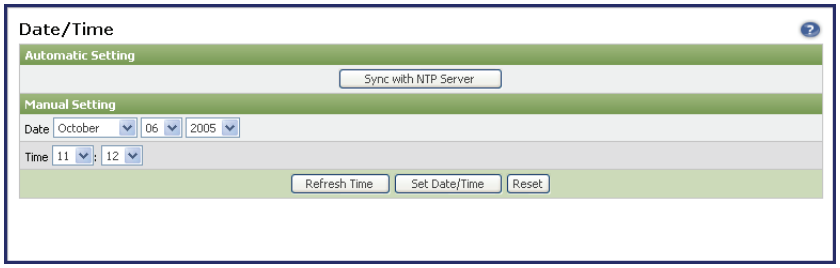
As is indicated on the screen, you have the option of gracefully shutting down only as much as necessary. The options on the screen define those features and functions that will be impacted by the restart process.

After IronMail is running, ***never*** press the reset switch on the front of the appliance until IronMail has been gracefully shut down from within either the graphical Web Administration or Command Line interface. Pressing the reset switch while IronMail is currently running forces IronMail to "hard boot" - a process that will corrupt its internal databases, and render it inoperable. Damage to IronMail's database will require CipherTrust's Technical Support engineers to manually repair and rebuild the corrupted files.

Setting the Date and Time

The displayed date and time reflects IronMail's internal date and time at the moment this page is opened or the **Refresh Time** button is clicked. If NTP time servers are entered in *System* > *Configuration* > *Appliances*, IronMail "syncs" itself with one of the servers once every minute.

System > Date/ Time



Manually adjust the time or date by specifying date and time values from the pick lists. After manually entering new values, click **Set Date/Time** to update IronMail.

If a time or date is entered *further ahead than the administrative inactivity time-out interval*, IronMail will log out all administrators currently logged onto the graphical user interface. Simply log back in and continue the administrative session as usual.

If the time is reset backward, administrators will be prompted to reboot the appliance in order for the setting to take effect.

WARNING: Extreme caution should be used whenever manually changing the internal IronMail time and date more than one minute from what the NTP time server is reporting. (If NTP server information was provided in IronMail's Configuration window, IronMail automatically synchronizes with the server once every minute.) Within the next minute after the time is manually changed, the automatic time server synchronization will reset IronMail's clock again.

Manually changing the internal clock more than one minute ahead or back ***will also affect IronMail's queues*** (e.g., Outbound Queue, Content Filtering Queue, etc.) and mail services (e.g., SMTPI Service, SMTPO Service, etc.). These processes all run on a "cycle time"—on average, several times a minute. After processing messages and before "going to sleep," they calculate the time stamp for when they will next "wake up" to process new messages. If the internal clock is moved forward one whole day, for example, the queues and services will instruct IronMail that their next "wake up" time is going to be tomorrow plus *nnn* seconds (where *nnn* = the real cycle time). However, one minute later, the time servers will re-sync IronMail's clock back to *today* without resetting IronMail's queues' and mail services' "wake up" time. The queues and services will wait until tomorrow to wake up and begin processing messages again. Therefore, if the clock is ever manu-

ally changed by more than one minute, always stop and restart each of the queues and services to reset their "wake up" times.

Force IronMail to immediately synchronize with an Internet Time (NTP) Server by clicking **Sync with NTP Server**. Note that the name of a valid time server must have entered in the *System* > *Configuration* > *IronMail* page to do this.

Note that IronMail writes a timestamp in its database noting when each message enters the Outbound Queue for delivery. IronMail uses this timestamp as a reference for when it may "pick up" messages for delivery. Therefore, if the clock is set backward and there are currently messages in the outbound queue, those messages' delivery will be delayed until IronMail's internal clock "catches up" to the time-stamp originally entered in the database.

Daylight Savings Time

IronMail automatically adjusts for Daylight Savings Time (DST) at 2 A.M. on the first Sunday of April and reverts to Standard Time at 2 A.M. on the last Sunday of October.

Storing CMC Keys

The Centralized Management option allows administrators to configure an IronMail appliance as a "slave" to another IronMail configured as a Centralized Management Console (CMC) "master." In enterprise environments with multiple IronMails protecting multiple domains and mail servers, centralized management allows an administrator to easily manage policies, push software and anti-virus file updates, as well as pull logs, reports, and alert messages.

Contact CipherTrust Sales to learn if Centralized Management Console architecture can aid in a particular enterprise email environment.

If an IronMail appliance is to be managed by a CMC, it must have the CMC's public key installed.

System > Store CMC Key

The Store CMC Key page contains a Browse button. Use it to navigate to the file containing the Centralized Management Console's (CMC) "public key" which the CMC Administrator exported and saved to disk. The master/slave connections can only be mediated though this public key. The key provides for encrypted sessions between the CMC and its slaves—a master and slave cannot communicate without it.

After navigating to and selecting the CMC's public key file, click **Store CMC Key** to install the CMC's public key.

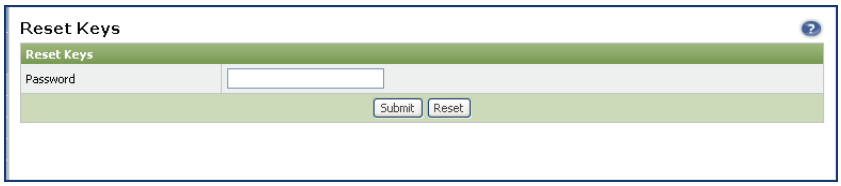
The **Reset** button clears the Browse navigation input field if Store CMC Key has not yet been clicked.

Resetting Keys

If an IronMail appliance breaks down due to unexpected events, and is not accessible online to CipherTrust Support, the appliance may be restored using a Recovery CD.

The following steps are required for restoring the IronMail appliance:

1. CipherTrust Support ships a Recovery CD to the customer.
2. The Administrator boots the IronMail appliance using the CD. The CD installs the fresh CTBSD (the customized operating system) on the IronMail, and the user is asked for the serial number of the IronMail appliance.
3. Support also mails the customer a temporary license, valid for 30 days. This license only enables the System tab in the IronMail interface. The license is generated using the default ct_maint key.
4. The Administrator runs the setup wizard. The license is required at this stage of the process.



5. The Administrator uses the screen shown above (*System > Reset Keys*) and the instructions that follow to create new keys for ct_maint, ct_upgrade and *cmc*. **Note:** This action will overwrite all default keys.
6. The Administrator downloads the encrypted file <serialnum>-keys.zip. The Administrator sends the downloaded file and the password used in creating the keys to CipherTrust Support.
7. Support places the new keys in operation by:
8. deciphering the setup file and replacing the old keys with the new ones
9. generating the new license using the new keys
10. emailing the new (permanent) license to the customer
11. The customer installs the new license, which enables all licensed features of IronMail, and, if a backup exists, restores the backup on the IronMail.

VIII: Additional Functions

Introduction

This portion of the User's Guide will provided descriptions of IronMail functions and features that fall outside the scope of the normal GUI approach to managing the system. The content may vary as functionality is added or modified.

In this section

In this section, you will find the following chapter:

- Chapter 15: The Command Line

Using the Command Line

In this chapter

In this chapter you will find information about the following topics:

- The Command Line
  - The Commands

The Command Line

IronMail allows the Administrator to access much of the functionality available through the Graphical User Interface (GUI) from the command line. The Administrator may access the command line through either of two methods:

- via the Console, which is a keyboard connected directly to the IronMail appliance, or
- from a workstation, using a Secure Shell (SSH).

Role management for the command line is accomplished at log-in. The user name and password the Administrator enters will be used to verify access rights and permissions.

From the Console:

If a keyboard and a monitor are connected to the IronMail appliance and the IronMail is currently running, the monitor shows a log-on prompt. The keyboard must be attached to the IronMail appliance before the appliance is powered on. After the Administrator enters a valid user name and password, the command functions may be accessed by typing simple commands.

The user name and password should generally be the same as those used for GUI access. It is important to remember that, unlike using GUI functions, the Administrator will NOT be logged off after a preconfigured period of time; the log-in remains active until the Administrator logs out. For security reasons, one should not walk away from the console without first logging out by typing ***exit*** at the command prompt.

From a Secure Shell:

The Administrator may also access the command line from a workstation that uses a Secure Shell application (via port 22). The Administrator logs in by entering a valid GUI user name and password.

If the appliance is an IronMail 210 or 345 model, each of which contains two Network Interface Cards (NICs), and if Out-of-Band Management is enabled, the hostname of the Out-of-Band NIC will be required to allow connection to the CLI. The IronMail 305 also has two NICs, but it does not support Out-of-Band Management.

SSH clients vary widely, and keyboard mapping is different from client to client. Depending upon which client you are using, you may be required to re-map the ***backspace*** key.

Once logged in, the Administrator is able to enter commands as necessary.

The Commands

Commands consist of a *command word* followed by one or more *parameters*. Separate the command word and the parameters from each other with a single space. Press Enter after the last parameter to execute the command. The information that appears in the CLI complies with any restrictions or parameters that have been configured in the GUI. Any restrictions or permissions applicable in the GUI also apply to the CLI. Furthermore, the amount of information in the IronMail's detailed logs viewed in the GUI is controlled by the logging level set in the IronMail GUI.

CipherTrust does not provide customers root access to the appliance; therefore, the CLI has limited shell capabilities. Many of the commands found in a UNIX environment are not available. Only the following commands may be executed:

help, edit, run, set, show, system, tail, and test.

The table below provides more information

Command Overview

Command	First-Level Parameter	Equivalent GUI Role	Access
help	edit, run, set, show, system, tail, test (plus additional parameters)		Typing **help** at the prompt displays commands and associated text. Typing **help** before any command word or command string displays help for that subset of the command line.
edit	interface route support	System System System	Read, Write Read, Write Read, Write

Command Overview

Command	First-Level Parameter	Equivalent GUI Role	Access
run	clean quarantine	Queue Manager	Read, Write
	clean message	Queue Manager	Read, Write
	reports	Reporting	Read Only
set	serial	System	Read, Write
	enable service	System	Read, Write
	disable service	System	Read, Write
	stop service	System	Read, Write
	start service	System	Read, Write
	user unlock	System	Read, Write
show	log	Reporting	Read Only
	mapping	Reporting	Read Only
	network	System	Read Only
	queue	Reporting	Read Only
	services	Reporting	Read Only
	system	System	Read Only
system	reboot	System	Read, Write
	restart	System	Read, Write
	restore	System	Read, Write
	shutdown	System	Read, Write
tail	log	Reporting	Read Only
test	dns	System	Read Only
	mail	System	Read Only
	ping	System	Read Only
	port	System	Read Only
	route	System	Read Only
	server	System	Read Only

The HELP Command

On-screen help may be accessed by typing **help**. If one types **help** at the IronMail command prompt, the screen will display the top-level commands that may be used (along with any associated help text). Typing **help** before any allowed command word (**edit**, **run**, **set**, **show**, **system**, **tail** or **test**) or command string (command word plus parameters) displays help for that subset of the CLI.

```
ironmail: help

Command Summary

The words appearing on the line below are the top level com-
mands. Type an individual word to see the parameters for that
command.  Type 'help <word>' to see help for that command.
```

help edit run set show system tail test

Commands are composed of a command word followed by one or more parameters. Separate the command word and parameters from each other with a single space. Press Enter after the last parameter.

On-screen help is available by typing 'help'. Typing 'help' before any command word displays help for that command. For some commands, typing 'help' before the command word and parameters can provide more information.

ironmail:

The simulated screen shot below displays the allowable parameters and help text for the **help edit** command.

ironmail: help edit

The EDIT command is used to edit network interface, routing table as well as enable or disable the support access feature.

Command Summary:

edit	interface	primary
		oob
	route	add
		delete
	support	enable
		disable

The EDIT Command

The **edit** command is used to modify specific configuration settings for the parameters **interface**, **route** and **support**. It impacts the way IronMail appears to and works with clients.

Examples showing the syntax for the edit command are shown in the simulated screen shot below.

Command Summary:

edit	interface	primary
		oob
		clearpending
	route	add
		delete
	support	enable
		disable

ironmail: edit interface primary

<PRIMARY> IP Address [10.50.1.234]

<PRIMARY> Netmask [255.255.255.0]

<PRIMARY> Select media type from the list, or press ENTER to use default:

0. Default
1. autoselect
2. 10baseT/UTP
3. 10baseT/UTP (full-duplex)
4. 100baseTX
5. 100baseTX (full-duplex)
6. 1000baseTX
7. 1000baseTX (full-duplex)

Media Type (0-7) [0]:

Warning! The setting will affect the way IronMail works with clients. Are you sure (Y/N) n

Change has been discarded.

The RUN Command

The **run** command allows the Administrator to execute specific commands at will. The two commands permitted are **run clean** (to clean *expired or deleted messages* in a quarantine queue, to clean *expired messages* in other queues) and **run reports** for a specified date. These commands may be configured within the GUI to execute on a daily basis without intervention, but the **run** command allows on-command execution.

Because it executes a complex SQL query of the IM database, the **run** command, whether for cleaning or reporting functions, will have a significant impact on overall performance. Therefore, this command should always be scheduled to run at a non-peak utilization period.

The simulated screen below shows the parameters and syntax for the **run clean** command string. The **run clean quarantine** command will clear or delete messages in the quarantine queue that have reached the time limit specified when the queues are configured. The **run clean message** command will clear or clean messages in other queues that have met the configured time limit.

Command Summary:

```
run     clean     quarantine
                  message
        reports   <MM/DD/YYYY>
```

ironmail: run clean quarantine

Forcing immediate clean-up will highly impact the performance of the appliance. Are you sure? (Y/N) n

Discarded the changes.

ironmail:

```
ironmail: run clean message

Forcing immediate clean-up will highly impact the performance of
the appliance. Are you sure? (Y/N)

Discarded the changes.

ironmail:
```

The parameters and syntax for the **run report** command are as shown below. The run report command will create all enabled reports from the Reports Configuration screen, with the exception of the Policy Configuration Report and the Vulnerability Assessment report, both of which are run only at the Administrator's discretion.

```
ironmail:

ironmail: run reports

*** Invalid command: Usage - run reports <MM/DD/YYYY> ***

ironmail:

ironmail: run reports 10/12/2004

Generating reports will highly impact the performance of the
appliance. Are you sure? (Y/N) n

No report job submitted.

ironmail:
```

The SET Command

The **set** command is used to start, stop, enable and disable IronMail services, to configure the serial port, and to unlock user accounts that have been locked due to excessive failed login attempts. The **set** command accepts three parameters: **serial**, **service**, and **user unlock**. Once the user enters the command and first parameter, the screen displays a list of sub-parameters.

```
Command Summary:
set     serial     cli
                   ups
          service  enable     <SERVICE>
                   disable    <SERVICE>
                   start      <SERVICE>
                   stop       <SERVICE>
        user       unlock     <USERNAME>
        <SERVICE> = IronMail Services:
                    smtpproxy, smtpsproxy, smtpo, pop3proxy
                    pop3sproxy, imap4proxy, imap4sproxy, etc.
      <USERNAME> = IronMail User Account
```

The **set serial** command configures IronMail's serial port to do one of two things: to allow connection of a keyboard (console) directly to the

appliance, using the **cli** sub-parameter; or to allow connection of an uninterruptable power supply, using the **ups** sub-parameter.

```
ironmail:
ironmail: set serial
*** Invalid command: Usage - set serial [cli|ups] ***

ironmail: set serial ups
The serial port is already set.

ironmail: set serial cli
Warning! The change may take up to 5 minutes ...
Serial port has changed.

ironmail: set serial ups
Warning! The change may take up to 5 minutes ...
Serial port has changed.
ironmail:
```

The **set service** command is used to enable, disable, start or stop an IronMail service.

Note: a disabled service cannot be started.

A service can also be disabled in the GUI by de-selected the Autostart option for that service.

```
ironmail:
ironmail: set service
*** Invalid command: Usage - set service [enable|disable|start|stop] ***
ironmail: set service enable
*** Invalid command: Usage - set service enable <SERVICE> ***
ironmail: set service disable
*** Invalid command: Usage - set service disable <SERVICE> ***
ironmail: set service start
*** Invalid command: Usage - server service start <SERVICE> ***
ironmail: set service stop
*** Invalid command: Usage - server service stop <SERVICE> ***
```

The set **user unlock <username>** command is used by the Administrator to unlock an appliance that has been locked due to circumstances like failed login attempts exceeding the maximum allowed. A valid username is required.

```
ironmail: set user
```

*** Invalid command: Usage - set user [unlock] ***

ironmail: set user unlock

*** Invalid command: Usage - set user unlock <USER ID> ***

ironmail:

The SHOW Command

The **show** command displays information about IronMail's system, services, network and logs. After the user types the command and the first parameter, the screen displays available sub-parameters.

Command Summary:

```
show    log     <SERVICE>
        mailroute
        network     connections
                    interface
                    route
        queue
        system      <SERVICE>
        services
        system      disk
                    process
                    support
```

To get more information on each of these commands, type 'help show log', 'help show services', or 'help show system'.

The **show log** command allows the Administrator to view today's logs, or those from a previous day.

ironmail: help show log

The 'show log' command is used to view today's, or previous days' logs. To see the list of services whose logs are available, type 'show log'.

To view today's logs for an individual service, type 'show log <SERVICE>' (where <SERVICE> is one of the services displayed by the 'show log' command). Appending a '?' after <SERVICE> displays the dates for previous days' logs. Appending the date after <SERVICE> displays the log for that day.

Examples:

show log smtpproxy = Show today's smtpproxy log

show log smtpproxy ? = Show dates for previous days' logs available

show log smtpproxy 20040101 = Show the smtpproxy log from 1/1/2004

ironmail:

ironmail: show log

```
show log
[ade|admin|alert|avq|cfq|cleanup|ct_admin|ct_audit|ct_euser|eus-
rquarant

ine|imap4proxy|imap4sproxy|ironwebmail|joinq|lda-
psync|mmq|pop3proxy|pop3sproxy|reports|ripq|sched|

schedftp|smtpol|smtpproxy|smtpsproxy|spamq|sshdct|sum-
mary|superq|vfq|watch] <Date, ? for list, Enter for today>
```

The **show mailroute** command displays information about the configured routing for various email protocols.

```
ironmail: show mailroute

*** Invalid command: Usage - show mailroute
<IMAP4|POP3|SMTP> ***

ironmail: show mailroute IMAP4

Protocol        Routing Domain  Routing Host

--------        --------------  ------------

IMAP4           DEFAULT         mail.x3.ctqa.net

IMAP4           x3.ctqa.net     mail.x3.ctqa.net

ironmail:
```

The **show network** command shows details about network configuration.

```
ironmail: help show network

The 'show network' command is used to view network related
information.

show    network connections

              interface

              route

ironmail: show network connections

Active Internet connections

Proto Recv-Q Send-Q  Local Address          Foreign Address
(state)

tcp4       0      0  localhost.22502       localhost.1212
ESTABLISHED

tcp4       0      0  localhost.1212        localhost.22502
ESTABLISHED

tcp4       0      0  localhost.3306        localhost.3218
ESTABLISHED

tcp4       0      0  localhost.3218        localhost.3306
ESTABLISHED

tcp4       0      0  localhost.3659        localhost.30340
TIME_WAIT
```

```
tcp4       0      0  im.1174               upd.ctqa.net.20022
TIME_WAIT
tcp4       0      0  localhost.22502       localhost.4192
TIME_WAIT
tcp4       0      0  localhost.2769        localhost.3306
TIME_WAIT
tcp4       0      0  localhost.22502       localhost.2688
TIME_WAIT
tcp4       0      0  localhost.2973        localhost.3306
TIME_WAIT
tcp4      74      0  im.4447               im.10443
CLOSE_WAIT
tcp4       0      0  localhost.8009        localhost.3337
ESTABLISHED
tcp4       0      0  localhost.3337        localhost.8009
ESTABLISHED
tcp4       0      0  localhost.8009        *.*                LISTEN
tcp4       0      0  im.https              *.*                LISTEN
tcp4       0      0  im.10443              *.*                LISTEN

ironmail:
ironmail: show network interface
<PRIMARY> interface
  Attribute     Current         Pending
  =========     =======         =======
  IP Address    10.50.1.234     None
  Netmasks      255.255.255.0   None
  Media Type    None            None
  Status        active          None
<OOB> interface DISABLED
  Attribute     Current         Pending
  =========     =======         =======
  IP Address    None            None
  Netmasks      None            None
  Media Type    None            None
  Status        no carrier      None
ironmail:
ironmail: show network route
No static route record.
ironmail:
```

The **show queue** command displays configuration information about processing order.

```
ironmail: show queue
    Queue Position and Name
    =======================
  1  Internal Queues - MIME Ripper
  2  Internal Queue - Content Extraction
  3  Super Queue
  4  Queue - Anti Spam
  5  Queue - Virus Scan
  6  Queue - Mail Monitoring
  7  Queue - Content Filtering
  8  Internal Queue - MIME Joining
  9  SMTPO Service
ironmail:
```

The **show services** command displays the current status of IronMail's services.

```
ironmail: show services
Mail Processes
Service          Auto-Start      Running       Uptime(D:H:M:S)
================================================================
IronWebMail          Y           Y          0000:00:02:17
SMTPI Service        Y           Y          0000:22:51:44
SMTPIS Service       Y           Y          0000:22:51:44
SMTPO Service        Y           Y          0000:22:51:44
POP3 Service         Y           Y          0000:22:51:44
POP3S Service        Y           Y          0000:22:51:44
IMAP4 Service        Y           Y          0000:22:51:44
IMAP4S Service       Y           Y          0000:22:51:43
Queue Processes
Service          Auto-Start      Running       Uptime(D:H:M:S)
================================================================
Super Queue          Y           Y          0000:00:00:31
Misc Processes
Service          Auto-Start      Running       Uptime(D:H:M:S)
================================================================
```

```
CLI Access                Y          Y          0000:22:51:44
CipherTrust Support Ac    Y          Y          0000:04:56:10
Alert Manager             Y          Y          0000:22:51:42
Network IDS               Y          Y          0000:22:51:43
Anomaly Detection Engi    Y          Y          0000:22:51:40
Internal Processes
Service                   Auto-Start Running    Uptime(D:H:M:S)
================================================
Int - Webadmin            Y          Y          0000:00:02:17
Int - Tomcat              Y          Y          0000:22:51:37
Int - Health Monitor      Y          Y          0000:22:51:39
Int - Reports             Y          Y          0000:12:27:05
Int - Scheduler           Y          Y          0000:22:51:42
Internal Queues - MIME    Y          Y          0000:22:51:42
Internal Queue - MIME     Y          Y          0000:22:51:42
Internal Queue - Conte    Y          Y          0000:22:51:42
ironmail:
```

The **show system** command string displays critical information about the IronMail system, including disk status and process statistics.

```
Command Summary:
show    system    disk
                  process
                  support


ironmail: show system disk
Mounted     Size    Used    Avail Capacity   iused    ifree  %iused
/ct          34G    1.3G     30G     4%    12129  8191645
0%
ironmail:


ironmail: show system process
Time    % User  % Sys  % Nice  % Intrpt  % Idle
00:00      5      0       0         0       95
00:01      6      0       0         0       94
00:04      3      2       0         0       95
00:05      3      2       0         0       95
00:06      4      0       0         0       96
00:06      4      2       0         0       94
```

```
00:07    4        1        0        1        95
00:08    5        1        0        0        94
00:09    7        0        0        0        93
ironmail:


ironmail: show system support
Support access is enabled.
Support access listen port has set to {port:20022}.
ironmail:
```

The SYSTEM Command

The SYSTEM command is used to reboot/shutdown IronMail and restore IronMail's factory settings. (You may restore either the security certificate, network settings, or disable ACL on the WebAdmin.) Restoring factory settings can be used to recover when the Graphical User Interface of IronMail's Web Administration has become unavailable due to misconfiguration.

The **system** command accepts the following parameters: **shutdown reboot restart restore**.

```
Command Summary:
To Reboot/Shutdown system: system reboot
                                    shutdown
To Restart Webadmin:  system restart webadmin
To Restore Factory Settings: system restore acl
                                          certificate
                                          network
```

The TAIL Command

The **tail** command shows a real-time view of all IronMail logs, beginning with the 10 most recent entries. The command accepts the parameter: **log** The tail command accepts no additional switches.

The **tail log** command accepts the additional parameters of the names of IronMail logs. Typing **tail log** will reveal a list of all available logs.

```
Command Summary:
tail    log  <SERVICE>
ironmail: tail log
tail log
[adeladminlalertlavqlcfqlcleanuplct_adminlct_auditlct_euserleus-
rquarantinelimap4proxylimap4sproxylironwebmaill
joinqlldap-
psynclmmqlpop3proxylpop3sproxylreportslripqlschedlsched-
ftplsmtpolsmtpproxylsmtpsproxylspamql
sshdctllsummarylsuperqlvfqlwatch] <Date, ? for list, Enter for
today>
```

```
ironmail:
ironmail: tail log cfq
Channel2::6:10122004 15:14:50:LOG_STAT_FINAL|6|PUSHED
TO NEXT Q
Channel3::7:10122004 15:15:20:LOG_STAT_ATT_FIL: {}
Channel3::7:10122004 15:15:20:LOG_STAT_CONT_FIL: {}
Channel3::7:10122004 15:15:20:LOG_STAT_FINAL|7|PUSHED
TO NEXT Q
Channel4::8:10122004 16:48:25:LOG_STAT_ATT_FIL: {}
Channel4::8:10122004 16:48:25:LOG_STAT_CONT_FIL: {}
Channel4::8:10122004 16:48:25:LOG_STAT_FINAL|8|PUSHED
TO NEXT Q
Channel5::9:10122004 17:05:07:LOG_STAT_ATT_FIL: {}
Channel5::9:10122004 17:05:07:LOG_STAT_CONT_FIL: {}
Channel5::9:10122004 17:05:07:LOG_STAT_FINAL|9|PUSHED
TO NEXT Q
```

The TEST Command

The **test** command is used to test network connections by using different methods, as well as to check specific server connections. The **test** command accepts the following parameters: **dns mail ping port route server**.

Examples are shown below:

```
Command Summary:
test    dns       forward <DNS SERVER IP> <HOSTNAME>
                  mx      <DNS SERVER IP> <DOMAIN NAME>
                  reverse <DNS SERVER IP> <IP ADDRESS>
        mail      <MAIL SERVER IP> <SENDER> <RECIPIENT>
        ping      <HOST>
        port      <IP ADDRESS> <PORT>
        route     <DOMAIN NAME>
        server    rlb <IP ADDRESS> <RBL SERVER> <DNS SERVER
IP> <QUEUE TYPE>
                  sls
                  update
ironmail:
ironmail: test server sls
# 10/13/04 11:42:01 EDT  /ct/apps/sls/client/conf/map
# Re-resolve names after 13:41:56  Check RTTs after 11:57:01
# 8000.00 ms threshold, -8000.00 ms average    1 total, 1 work-
ing addresses
```

```
IPv6 off
sls1.ciphertrust.net,-123789 client101
# * 10.50.1.16,-qa1.DCC.ciphertrust ID 1040
#     100% of 32 requests ok    10.85 ms RTT 6 ms queue wait
```

The History Command

The history command will display a list of previously run commands. You can execute a previous command listed in the history by prefixing the number from the list with an exclamation point.

Examples are shown below:

```
ironmail:
ironmail: history
    1   history
    2   show network interface
    3   history
    4   history
    5   show log
    6   show log admin
    7   history
    8   show queue quarantine
    9   history
```

!*n* executes command n from the top.

!-*n* executes commands from the bottom.